

University of Newcastle upon Tyne
Faculty of Science, Agriculture and Engineering
School of Computing Science

Certificate Validation in Untrusted Domains

Ph.D. Thesis

By

Omar Abdullah Batarfi

NEWCASTLE UNIVERSITY LIBRARY

205 36727 1

Thesis L8457

**A thesis submitted in partial fulfilment
of the requirements for the degree of**

Doctor of Philosophy

April 2007

**TEXT
BOUND INTO THE
SPINE**

ABSTRACT

Authentication is a vital part of establishing secure, online transactions and Public key Infrastructure (PKI) plays a crucial role in this process for a relying party. A PKI certificate provides proof of identity for a subject and it inherits its trustworthiness from the fact that its issuer is a known (trusted) Certification Authority (CA) that vouches for the binding between a public key and a subject's identity.

Certificate Policies (CPs) are the regulations recognized by PKI participants and they are used as a basis for the evaluation of the trust embodied in PKI certificates. However, CPs are written in natural language which can lead to ambiguities, spelling errors, and a lack of consistency when describing the policies. This makes it difficult to perform comparison between different CPs.

This thesis offers a solution to the problems that arise when there is not a trusted CA to vouch for the trust embodied in a certificate. With the worldwide, increasing number of online transactions over Internet, it has highly desirable to find a method for authenticating subjects in untrusted domains.

The process of formalisation for CPs described in this thesis allows their semantics to be described. The formalisation relies on the XML language for describing the structure of the CP and the formalization process passes through three stages with the outcome of the last stage being 27 applicable criteria. These criteria become a tool assisting a relying party to decide the level of trust that he/she can place on a subject certificate. The criteria are applied to the CP of the issuer of the subject certificate.

To test their validity, the criteria developed have been examined against the UNCITRAL Model Law for Electronic Signatures and they are able to handle the articles of the UNCITRAL law.

Finally, a case study is conducted in order to show the applicability of the criteria. A real CPs have been used to prove their applicability and convergence. This shows that the criteria can handle the correspondence activities defined in a real CPs adequately.

PUBLICATIONS

Parts of this thesis have been published as follows:

- 1 Batarfi, O., Certificate Validation in Untrusted Domains. On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASEOTM, OTM 2003 Workshops. Catania, Sicily, Italy, 3-7 November 2003. Lecture Notes in Computer Science, Springer Verlag Publishers, Volume 2889 pp. 1057 - 1068.
- 2 Batarfi, O., ATV: An Efficient Method for Constructing a Certification Path. 18th IFIP World Computer Congress. Toulouse, France, 22-27 August 2004. Kluwer Academic Publishers, Volume 11 pp. 67 - 74.
- 3 Batarfi, O., Snow, C. R. An Approach to the Formalisation of a Certification Policy. Technical report CS-TR: 918. The University of Newcastle upon Tyne, School of Computing Science, Jul 2005.

Also it was accepted as a poster in the 7th Intl Symposium on System and Information Security SSI'2005. Sao Paulo, Brazil. 08-11 November 2005.
- 4 Batarfi, O., Marshall, L. Defining Criteria for Rating an Entity's Trustworthiness Based on Its Certificate Policy. The First International Conference on Availability, Reliability and Security, Dependability and Security in e-Government Workshop

(DeSeGov 2006). Vienna, Austria, 20-22 April 2006. IEEE Computer Society, pp.

996 – 1003.

- 5 Batarfi, O., Marshall, L. Conformance Testing a Set of Criteria for Assessing Trust. Journal of Computers (JCP), Academy Publisher. Volume : 2 Issue: 1 February 2007.

<http://www.academypublisher.com/jcp/vol02/no01/jcp02014449.pdf>

ACKNOWLEDGEMENTS AND DEDICATION

I praise God almighty for all blessings that I have received to fulfil my ambition. Secondly, I would like to thank my supervisors Dr. Richard Snow and Dr. Lindsay Marshal for their invaluable support and academic guidance during my research work. I consider myself extremely fortunate and privileged to have been supervised by them. Their way in supervision gave me a much freedom as I wanted in the work which has instilled me in a sense of responsibility and as strong work ethic. I feel grateful to Dr. Lindsay that he accepted to be my supervisor since Dr. Snow has retired, and for his careful revision of my thesis.

I would like to extent my gratitude to my committee, Prof. Peter Ryan and Dr. Aad van Moorsel, for their insightful comments and suggestions on my research during the regular thesis committee meetings. I would like to show my gratitude to all members of the School of Computing Science who tremendous emotional supports especially Dr. John Lloyd head of the school for giving me a wonderful opportunity to attend conferences.

My most profound gratitude goes to my wife who stands alongside me, sharing both joys and sorrows. Also I would like to thank my five kids who have been the timeless source of inspiration for me with their favourite daily question "When are you going to finish the thesis dad?" Special thanks also go to my mom who continually remembers and prays for me, whose importance I shall not try to put into words.

I would like to thank also King Abdulaziz University for their generous scholarship.

Finally, I dedicate this thesis to my father Abdullah Batarfi, who could not wait to see me accomplish his dream.

TABLE OF CONTENTENS

CHAPTER 1	1
INTRODUCTION	1
1.1 Background	1
1.2 Security Concepts	4
1.2.1 Encryption.....	4
1.2.2 Cryptography	4
1.2.3 Public-key Cryptography.....	5
1.3 Public key Infrastructure.....	6
1.4 Trust.....	7
1.4.1 Single Trust Domain.....	10
1.4.2 Joined Trust Domains.....	10
1.5 Motivation	11
1.6 Our Approach	12
1.7 Related Work	14
1.7.1 Formalisation	14
1.7.2 Comparison.....	15
1.8 Thesis Structure	16
CHAPTER 2	19
SECURING TRANSACTIONS ON THE INTERNET.....	19
2.1 Introduction.....	19
2.2 Public Key Infrastructure.....	19
2.3 PKI Standards.....	21
2.3.1 X.509	21
2.3.2 PKIX.....	22
2.4 PKI Services	22
2.4.1 Authentication.....	22
2.4.2 Encryption.....	23
2.4.3 Integrity.....	23
2.4.4 Non-repudiation.....	23
2.5 PKI Architecture	23
2.5.1 Hierarchical Architecture.....	24
2.5.2 Mesh Architecture	24
2.5.3 Single Architecture	25
2.6 Connecting Architectures	26
2.6.1 Cross-certification.....	26
2.6.2 Bridge CA	26
2.7 PKI Components.....	27
2.7.1 Certification Authority.....	27
2.7.2 Registration Authority	28
2.7.3 End-entity (Subscriber).....	28
2.7.4 Relying Party	28
2.7.5 Repository	28
2.7.6 X.509 Version 3 Certificate.....	36
2.8 Certificate Issuance	42
2.9 Certificate Revocation	43
2.10 The Certificate Validation Process.....	44

2.10.1	Evaluating Certification Paths During Path Construction	45
2.10.2	Direction of Path Construction	45
2.10.3	Problems with Certification Path Construction	46
2.10.4	Related work in Validating Certificate	47
2.10.5	Constructing Certification Paths with ATV	50
2.11	Conclusion	53
CHAPTER 3		55
CERTIFICATE POLICY TECHNIQUES FOR MEASURING TRUST		55
3.1	Introduction.....	55
3.2	Certificate Policy.....	56
3.2.1	A Certificate Policy Example	57
3.2.2	Object Identifiers	58
3.3	X.509 Certificate Fields	58
3.3.1	Certificate Policies Extension.....	58
3.3.2	Policy Mappings Extension	58
3.3.3	Policy Constraints Extension.....	59
3.4	Certification Practice Statement	59
3.6	Certificate Policy Framework	61
3.7	Contents of CP or CPS	62
3.8	Major considerations.....	64
3.9	Conclusion	64
CHAPTER 4		66
DEVELOPMENT OF THE FORMALISATION METHOD		66
4.1	Our Approach	66
4.2	First Version of the Formalisation	67
4.2.1	Applying the formalisation process	68
4.2.2	Testing the Formalisation	74
4.3	Second version of the formalisation	74
4.3.1	Representing Semantics.....	74
4.3.2	Obligation Title.....	75
4.3.3	Formalisation Conventions.....	77
4.3.4	Tree Representation	79
4.3.5	Implementation.....	80
4.3.6	Testing the formalisation	101
4.4	Final version of the formalisation	101
4.4.1	Defining criteria for the comparison process.....	101
4.4.2	Comparison criteria for the formalisation.....	102
4.4.3	Requirements for certification service providers.....	104
4.5	Conclusion	109
CHAPTER 5		110
REPRESENTING THE CRITERIA IN THE XML FORMALISATION		110
5.1	Introduction.....	110
5.2	The Semantics behind the Criteria	110
5.2.1	Liability and Capability of the Subject (criterion 1).....	110
5.2.2	Allowance For RA to Issue Certificate (criterion 2)	111
5.2.3	Financial Cover (criterion 3)	111
5.2.4	National Law Enforcement (criterion 4).....	111
5.2.5	Dispute Reference (criterion 5)	112
5.2.6	Service Assessment (criterion 6)	112
5.2.7	Frequency of Service Assessment (criterion 7).....	113

5.2.8	Action on Deficiency (criterion 8).....	113
5.2.9	Confidentiality of Personal Information (criterion 9).....	114
5.2.10	Authentication of Organization Identity (criterion 10).....	114
5.2.11	Authentication of Individual Identity (criterion 11).....	115
5.2.12	Informed Subject (criterion 12)	115
5.2.13	CRL Update Interval Time (criterion 13).....	116
5.2.14	Validity Period of a CRL (criterion 14).....	116
5.2.15	Comprehensive Security Audit.....	116
5.2.16	Security Audit Log Examination (criterion 16).....	117
5.2.17	Vulnerability Assessment (criterion 17).....	117
5.2.18	Archiving Procedure (criterion 18).....	118
5.2.19	Disaster Recovery Plan (criterion 19).....	118
5.2.20	Trusted Roles (criterion 20).....	118
5.2.21	Personnel Controls (criterion 21).....	119
5.2.22	Subject Keys (criterion 22).....	119
5.2.23	Private Key Length (criterion 23).....	119
5.2.24	Keys validity period (criterion 24)	119
5.2.25	CA Machine Security (criterion 25)	120
5.2.26	Maintaining Hardware and Software Integrity (criterion 26).....	120
5.2.27	Network Security (criterion 27).....	120
5.3	Representing the Criteria in the Formalisation	120
5.3.1	Testing Liability and Capability of the Subject.....	121
5.3.2	Prohibiting RA from Issuing Certificates.....	121
5.3.3	Providing Financial Insurance	122
5.3.4	Enforcing National Law Superiority	123
5.3.5	Allowing For Arbitration in Cases of Dispute.....	123
5.3.6	Performing Compliance Audit.....	124
5.3.7	Performing Frequent Compliance Audit	124
5.3.8	Taking Action on Deficiency.....	125
5.3.9	Prohibiting A CA from Ever Disclosing Any Subject Confidential Information ..	126
5.3.10	Organization Authentication Should Include Organization's Reputation...	126
5.3.11	Authenticating the Identity of an Individual in Person.....	127
5.3.12	Informing the Subject of Rights and Obligations	127
5.3.13	Updating the CRL Immediately on Certificate Revocation	128
5.3.14	Issuing Frequent CRLs	128
5.3.15	Performing Comprehensive Security Audit.....	129
5.3.16	Examining Audit Logs Frequently	131
5.3.17	Performing Vulnerability Assessment.....	131
5.3.18	Providing Extensive Archiving.....	132
5.3.19	Establishing a Disaster Recovery Plan	133
5.3.20	Supporting Trusted Roles	134
5.3.21	Personnel Controls.....	135
5.3.22	Subject Generates Its Own Key Pairs.....	136
5.3.23	Minimum Length of the Private Key.....	136
5.3.24	Key Validity Periods.....	137
5.3.25	Protection of the CA Machine against Unauthorized Access.....	137
5.3.26	Checking the Integrity of the Hardware and Software	138
5.3.27	Securing Networks.....	139
5.4	Measurable Criteria	140
5.4.1	Scoring System	141

5.5 Comparison Result	144
5.5.1 No Overlap.....	144
5.5.2 Absolute Overlap	145
5.5.3 Partial Overlap	145
5.6 Acceptable Case	146
5.7 Conclusion	146
CHAPTER 6	148
COMPARISON OF CRITERIA WITH REQUIREMENTS	148
6.1 Introduction.....	148
6.2 UNCITRAL Model Law on Electronic Signatures.....	148
6.2.1 Article 6. Compliance with a Requirement for a Signature.....	150
6.2.2 Article 8. Conduct of the Signatory.....	152
6.2.3 Article 9. Conduct of the Certification Service Provider	153
6.2.4 Article 10. Trustworthiness	156
6.3 Conclusion	159
CHAPTER 7	160
CASE STUDY.....	160
7.1 Introduction.....	160
7.2 Criteria Formalisation.....	160
7.3 GlobalSign Certification Authority CP	161
7.4 Authenticating the GlobalSign CP	161
7.4.1 Compliance with Criterion 1	162
7.4.2 Compliance with Criterion 2	163
7.4.3 Compliance with Criterion 3	164
7.4.4 Compliance with Criterion 4	165
7.4.5 Compliance with Criterion 5	166
7.4.6 Compliance with Criteria 6.....	166
7.4.7 Compliance with Criteria 7.....	167
7.4.8 Compliance with Criterion 8	168
7.4.9 Compliance with Criterion 9	169
7.4.10 Compliance with Criterion 10	170
7.4.11 Compliance with Criterion 11	171
7.4.12 Compliance with Criterion 12	172
7.4.13 Compliance with Criterion 13	173
7.4.14 Compliance with Criterion 14	174
7.4.15 Compliance with Criterion 15	175
7.4.16 Compliance with Criterion 16	176
7.4.17 Compliance with Criterion 17	177
7.4.18 Compliance with Criterion 18	177
7.4.19 Compliance with Criterion 19	179
7.4.20 Compliance with Criterion 20	179
7.4.21 Compliance with Criterion 21	180
7.4.22 Compliance with Criterion 22	182
7.4.23 Compliance with Criterion 23	183
7.4.24 Compliance with Criterion 24	184
7.4.25 Compliance with Criterion 25	184
7.4.26 Compliance with Criterion 26	185
7.4.27 Compliance with Criterion 27	186
7.5 Authentication Result.....	187
7.5.1 Result Discussion.....	189

7.6 Conclusion 189

CHAPTER 8 191

CONCLUSIONS AND FUTURE WORK..... 191

8.1 Discussion 191

8.2 Future Work..... 197

8.2.1 Representing CPs Context More Systematically 197

8.2.2 Automating the Comparison..... 198

8.2.3 The Criteria Developed..... 199

8.2.4 Scoring System 199

8.2.5 Acceptance of Our Contribution..... 199

8.3 Closing Remarks 199

REFERENCE 201

Appendix A..... 207

KEY WORDS FOR USE IN RFCS TO INDICATE REQUIREMENT LEVELS... 207

Appendix B 209

TABLE TO PERFORM A MANUAL COMPARISON PROCESS 209

Appendix C..... 213

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)..... 213

LIST OF FIGURES

FIGURE 1-1 X.509 CERTIFICATE.....	6
FIGURE 1-2 PKI ELEMENTS.....	7
FIGURE 1-3 SECURE WEBSITE	9
FIGURE 1-4 RELYING PARTY AND THE SUBJECT IN THE SAME DOMAIN	10
FIGURE 1-5 RELYING PARTY AND THE SUBJECT IN DIFFERENT DOMAINS	11
FIGURE 1-6 CRITERIA PATH	13
FIGURE 2-1 HIERARCHICAL ARCHITECTURE.....	24
FIGURE 2-2 MESH ARCHITECTURE.....	25
FIGURE 2-3 SINGLE ARCHITECTURE	26
FIGURE 2-4 X.509 CERTIFICATE FORMAT	38
FIGURE 2-5 NAME CONSTRAINTS SCENARIO	51
FIGURE 2-6 POLICY PROCESSING SCENARIO	52
FIGURE 4-1 USING XML SCHEMA TO PERFORM COMPARISON	69
FIGURE 4-2 TREE PRESENTATION OF THE CA OBLIGATION SECTION.....	79
FIGURE 4-3 TREE PRESENTATION OF THE TWO DIFFERENT CPS	80
FIGURE 4-4 FIRST PAGE OF THE TABLE USED TO DO MANUAL COMPARISON PROCESS	102
FIGURE 5-1 NO OVERLAP CASE.....	144
FIGURE 5-2 ABSOLUTE OVERLAP CASE.....	145
FIGURE 5-3 PARTIAL OVERLAP CASE.....	145

LIST OF TABLES

TABLE 2-1 DIRECTORY ATTRIBUTES 30

TABLE 2-2 STANDARD EXTENSIONS 42

TABLE 2-3 PRIVATE INTERNET EXTENSIONS..... 42

TABLE 3-1 NINE COMPONENTS WITH THEIR SUBCOMPONENTS 63

TABLE 4-1 THE CRITERIA THAT WERE PRODUCED BY THE MANUAL COMPARISON
PROCESS..... 103

TABLE 4-2 SHOWING THE RELATION BETWEEN REQUIREMENTS AND CRITERIA..... 106

TABLE 4- 3 SHOWING THE NEW RELATION BETWEEN REQUIREMENTS AND CRITERIA
..... 107

TABLE 5-1 THE SCORING SYSTEM 141

TABLE 6-1 CORRESPONDENCE BETWEEN THE DEVELOPED CRITERIA AND THE
UNCITRAL LAW ARTICLES..... 158

TABLE 7-1 VERISIGN CP AUTHENTICATION..... 189

CHAPTER 1

INTRODUCTION

1.1 Background

Electronic information appears in our daily life in different forms, and we know how important it is in making our lives more convenient and manageable. Both individuals and organizations have benefited from the presence of electronic information and it plays a role in developing different ways of communicating between people, organizations and government sectors. The Internet is a prime example of the electronic information revolution and today its cover extends globally with around 300 million people accessing it. However, it is an open environment and insecure [1]. Certainly, the Internet can be considered as a revolution in computing and communication. It assists in opening private networks to the world and allows access by anonymous users. A number of factors have helped to make the Internet popular, perhaps the most important being the availability of tools that support accessing and obtaining services across it (e.g. web browsers). The Internet offers its many services twenty four hours a day, seven days a week and wide accessibility, ease of use, affordability and availability help in allowing people to adapt to this revolutionary technology. Nowadays people depend on the Internet to accomplish their work in areas such as:

- Finding news and information.
- Buying and selling goods.
- Arranging meetings.
- Sending documentation and other files.
- Publishing information.

The Internet is medium for collaboration between different entities and this new paradigm for the Internet highlights the necessity for security. The Merriam-Webster Dictionary [2] defines security as “the quality or state of being secure” or “freedom

from fear or anxiety”. Any secure system should preserve integrity, confidentiality and availability [3].

- Integrity: prevention of undetected unauthorized modification of information.
- Confidentiality: prevention of unauthorized disclosure or compromise of information.
- Availability: prevention of unauthorised withholding of information or resources.

Any deficiencies in the security of a system can increase exposure to security threats, such as security breaches. A threat is any potential danger to an information system that exploits a vulnerability to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse [4]. The best known security threats are impersonating a user or system, eavesdropping, denial of service, packet replay and packet amendment. In the following we, briefly summarize definitions of these threats:

- Impersonating a user (or system) is where a malicious user pretends to be another, legitimate network user.
- Eavesdropping is the interception of network activity to gain sensitive information such as passwords or procedures for performing functions and data.
- Denial of service is where an attacker disables systems on a network to prevent legitimate users from using them.
- Packet replay is where an attacker replies with an authentication sequence to gain access to a system after the intruder records and re-transmits message packets on the network.
- Packet modification involves an attacker intercepting and modifying packet contents before transmitting them to their original destination.

Threats to security are increasing, as every day we hear new fraud stories, and the majority of these frauds take place using the Internet. In the 2003 Survey of Fortune 1000 Companies, it was shown that Internet/Intranet security occupies third place

amongst all threats facing corporate America. Internet/Intranet fraud has moved in ranking from number 10 in 1997 to number 3 in 2003 [5]. Moreover, the Harris Interactive Survey of Fortune 1000 Companies reveals serious deficiencies in disaster preparation, where 36% of C-suite executives consider that hackers are the biggest threat to business-critical information [6].

A survey of UK businesses, Information Security Breaches Survey 2006, [7] shows that security threats are still a major worry for UK companies despite the number of companies that have actually experienced security incidents in 2006 coming down to 62% from 74% two years ago. The survey shows that the number of UK businesses using the Internet increased to 97% in 2006 from 93% in 2004. One of the survey's surprises was that despite all this information, two fifths of business are still allocating less than 1% of their IT budget to information security whilst the average cost associated with a security incident was £10,000 in 2004 but has increased in 2006 to £12,000.

The following quotation outlines the major problem of Internet vulnerabilities:

"The tremendous risk exposure resulting from successful attacks and the globalization of threats continue to make cyber security a boardroom-level issue. More than ever, organizations are relying on their technology infrastructure to conduct business. The complexity of the IT infrastructure and the lack of integration between security technologies continue to result in major vulnerabilities for organizations worldwide. It is only through sound security management that companies will successfully face the cyber risk in the 21st century." Russ Artzt, Executive Vice-President, eTrust Security Solutions, Computer Associates.

Finally, it is generally accepted that security is necessary for applications operating in distributed and open environments such as the Internet where its aim is to provide protection against threats to the communication of information.

1.2 Security Concepts

As we have just stated, security is a core requirement for any transaction over the Internet where parties who were previously unknown to each other can establish connections between themselves. All participants are therefore looking for some kind of assurance and have concerns about the trustworthiness of the other party. In fact, they are looking for some kind of evaluation of the other's trustworthiness. Finding a way to demonstrate trustworthiness to each other is considered a primary goal in an open environment such as the Internet. Trustworthiness becomes strengthened when essential security properties, integrity, confidentiality and authentication are satisfied [8]. Authentication is important in the age of faceless e-commerce, authentication assists the receiver of a digital message to be confident in both the identity of the subject and the integrity of the message [9]. Authentication is usually achieved using encryption where encryption of data enables the identity of both the sender and the receiver to be established. Of course, encryption satisfies the confidentiality property by preventing unauthorized access to data.

1.2.1 Encryption

Encryption of data that travels over the Internet is considered an adequate solution to protecting its privacy, i.e. it prevents the data from being intercepted during the transaction process. Encryption is defined in [10] as:

Any procedure used in cryptography to convert plaintext into ciphertext (an encrypted message) in order to prevent any but the intended recipient from reading that data.

As the definition states, encryption is a part of the field of cryptography.

1.2.2 Cryptography

Cryptography consists of encryption and decryption: converting ciphertext to plaintext ("original data"). The art behind cryptography is rendering data impossible to read without the knowledge of some secret key. This secret key is given with the

plaintext to an algorithm to produce the ciphertext. There are two types of cryptography depending on the key, or secret key: symmetric and asymmetric.

1.2.2.1 Symmetric Cryptography

Symmetric cryptography, also called secret key cryptography, is based on the pre-agreement of a shared secret key between the communicating parties. Once this agreement has been reached, the parties can start to communicate. The success of this kind of cryptography is dependant on the key remaining secret to everyone except the communicating parties, and for this reason, using a secure channel for establishing the shared secret key is essential [11]. The secret key is only to be used in the encryption and decryption of messages. Symmetric cryptography was commonly used until 1970 [11] and is still used today when appropriate.

1.2.2.2 Asymmetric Cryptography

Asymmetric cryptography eliminates the need to use a shared secret key and replaces it with the use of two keys, one called the “private key” and the other called the “public key”. The relationship between them appears as a completion role. Messages that have been encrypted with the public key will not decrypt unless the related private key is used. Only the private key needs to be kept secret by its owner and is not shared with others. Because of the design of the methods, it is impractical to compute the private key from the public key [11]. The public key is published freely, and is needed to communicate securely with its owner. Therefore, there is no need for a secure communication channel for the purpose of exchanging keys [11]. Asymmetric cryptography is also called Public-key cryptography.

1.2.3 Public-key Cryptography

The idea of using a public key to eliminate the need for secure key exchange has allowed Public-key cryptography to gain much publicity. Moreover, within a Public key Infrastructure, Public-key cryptography is also used to perform authentication and to create digital signatures as well as for encryption [11].

1.3 Public key Infrastructure

In [12] a Public key Infrastructure (PKI) is defined as:

a system that facilitates the distribution of public keys for Public-key cryptography. It is an infrastructure to provide a secured environment to transfer data from one point to another, with allowed and verifiable identity. As there are many security infrastructures available, PKI provides us with a cohesive set of procedures and services to conduct a secured transaction. The PKI provides a complete life cycle management system in handling keys and certificates.

As this definition states, PKI is a complete solution for handling transactions in a secure way, including the ability to verify the identity of the participants. It provides authentication, integrity and confidentiality for participants who are exchanging data through the Internet. Public and private keys are linked to the owner's identity through the public key certificate (most commonly an X.509 certificate), hereafter referred to simply as a certificate. Figure 1-1 shows an example of a certificate.

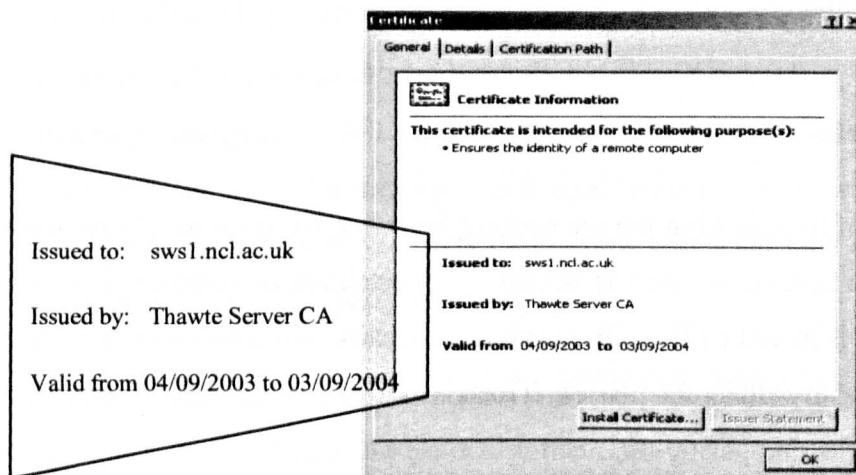


Figure 1-1 X.509 Certificate

A certificate is a proof of identity or a letter of authorization signed by an authoritative entity (the certificate issuer). The issuer of the public key certificate, the Certification Authority (CA), vouches for this identity after a Registration Authority (RA) verifies the subject's identity. A certificate could be issued to an end-user, a

device, Web server, process, or another CA. Figure 1-2 shows the major elements of a PKI.

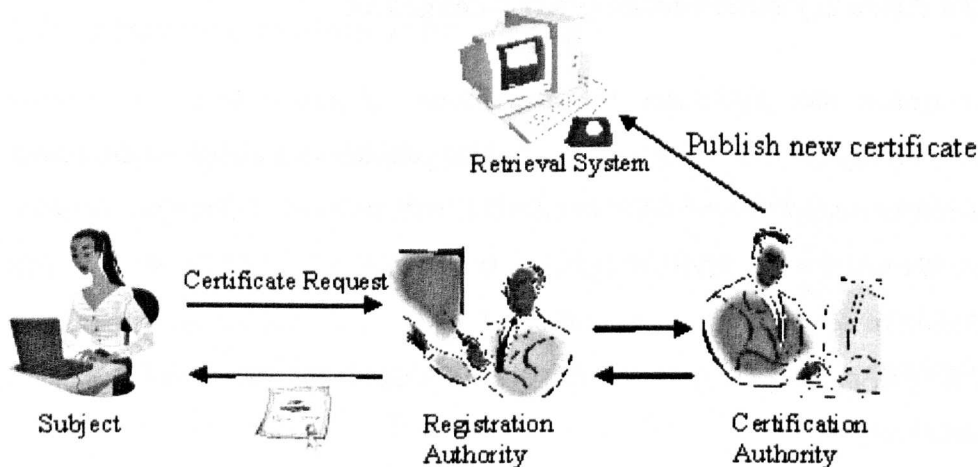


Figure 1-2 PKI Elements

The PKI lets companies take advantage of the speed, versatility, availability, immediacy and global access of the Internet whilst helping protect critical information from interception, tampering, and unauthorized access. The PKI assures the trustworthiness of public key-based security mechanisms : the confidentiality of private keys and the integrity of public keys [13].

1.4 Trust

A measure of trust is what we are looking for when we want to rely on someone, and in electronic commerce trust is necessary to establish confidence. It is important to clarify what is meant by trust in this context because different definitions of trust have been adopted by different people. Trust is defined in the ITU-T Recommendation X.509 specification [X509-00, Section 3.3.54] as:


Generally, an entity can be said to “trust” a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects.

Trust in the PKI is the result of the interplay of three major concepts: authentication, encryption and a CA [9].

A CA provides a level of assurance that the public key contained in a certificate does indeed belong to the subject whose identity is being associated with that key. The CA signs the public key certificate of the subject to provide the cryptographic binding between the subject's public key, her name, and other information in the certificate. When a recipient of a public key wants to determine whether a legitimate CA issued a certificate, he has to verify the issuing CA's signature on the certificate [9].

A PKI certificate enables Secure Socket Layer (SSL) technology, which allows the establishment of secure channels between a seller's server and a customer's browser. SSL provides the following secure online transactions [9]:

- **Authentication** – Customers can verify that the site belongs to the seller and not to anyone else. This assurance will boost their confidence when disclosing confidential information.
- **Message privacy** – All information exchanged between the seller's web server and a customer is encrypted and cannot be read, deciphered or decrypted by a third party that taps into the data being exchanged after the connection has been established.
- **Message integrity** – SSL uses a message digest mechanism to detect when the contents of a message have been tampered with, which ensures both parties involved in the transaction know that what they are seeing is exactly what the other party sent.

When SSL encryption technology is activated, a small lock () is displayed in the status bar of most web browsers. Additionally, the URL in the address box begins with “https://” instead of just “http:// “. Figure 1-3 depicts this technique.

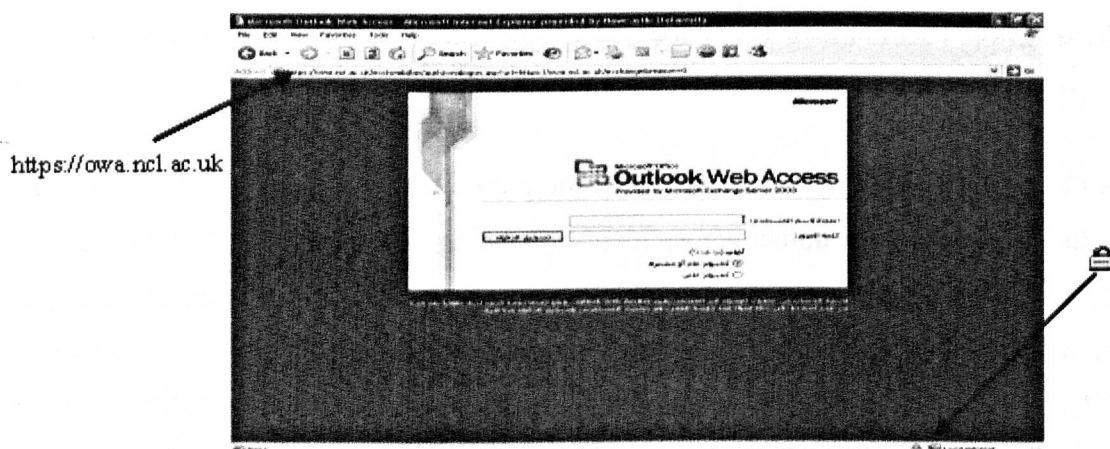


Figure 1-3 Secure Website

Every CA adheres to a policy, called the Certificate Policy (CP) which defines issues related to certificates such as the certificate community, applicability, liability, entities, etc. The CA is always the validator for the certificate if a relying party¹ wishes to check if a certificate is valid or not. This process is called *certificate validation*.

In [15], certificate validation is defined as:

the process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time.

A certification path is built from a trusted anchor, a CA trusted by the relying party, to the subject certificate. When processing a certification path, a CP that is acceptable to the relying party application must be present in every certificate in the path. The PKI model is based on trust : trust that certificates are issued by a trusted third party (CA), trust that a certificate represents a valid binding of a subject's identity, trust that private keys are kept safely, and trust that invalid certificates have been properly invalidated or revoked [16]. The trust anchor is trusted by the relying party, which leads to the fact that the relying party trusts any certificates the trust anchor issues

¹ As defined in 14. A. Arsenault and S. Turner. *Internet X.509 Public Key Infrastructure: Roadmap*. 2002 July [cited; 57]. "A user or agent that relies on the data in a certificate in making decisions".

[17]. A CA issues certificates to entities which adhere to its CP and they have some kind of connection between them. A domain is defined in [18] as the environment that connects nodes (CAs and end-entities) together. This leads us to conclude that the issuer CA simply creates a domain that includes all its certificates. If we apply this to the trust anchor, we see that the trust anchor really creates only a single trust domain for its relying parties. Moreover, the trust anchor could expand the trust to another CA domain by certifying it, we call this a "joined trust domain".

1.4.1 Single Trust Domain

A single trust domain is where PKI entities operate under the same CP; therefore, the relying party and the subject are in the same domain, as shown in figure 1-4:

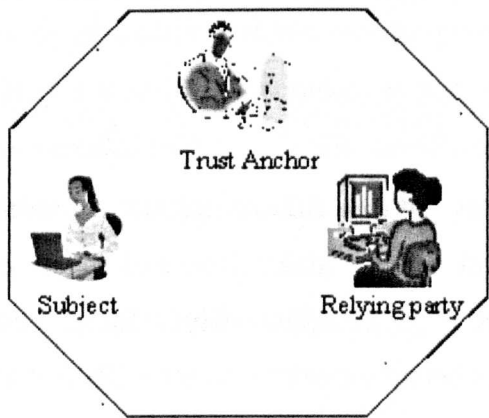


Figure 1-4 Relying Party and the Subject in the Same Domain

1.4.2 Joined Trust Domains

Here, two or more trust domains are joined together. In this case we could find that there is more than one CP operating. This issue has been sorted out by the CAs' acceptance of each others CP. Therefore, it is possible for the relying party to be in one domain and the subject in another. Figure 1-5 shows this case:

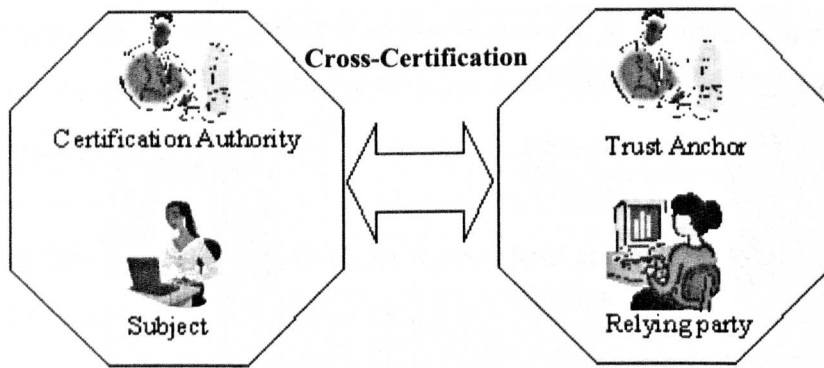


Figure 1-5 Relying Party and the Subject in Different Domains

Joining of domains is done by cross-certification, where each CA issues a certificate to the CA in the other domain, or by using the bridge technique where a mediator CA, or bridge CA, introduces each domain to another. This is accomplished through cross-certification between the bridge CA and each domain individually [11].

1.5 Motivation

The Internet reaches all over the world and provides valuable services. There are no barriers between information: it all looks alike, and the only difference sometimes is in the written language. This paradigm allows for powerful, easy and attractive services. The Internet has become essential to our daily life and there are many goods produced in different countries with low prices that we can purchase over the Internet. To buy these goods is an easy task which only requires you to provide the company's site with your credit card number. But before we do this we need to verify the site's trustworthiness in order to decide how much trust we can place on it and the company.

Each web browser has been initialised with predefined lists of CAs, and users can add or remove CAs from these lists. Note that [19] asserts that the built-in lists of CAs in Netscape and Microsoft browsers are not reliable although they have commonly been accepted as dependable. The user will be notified if the browser receives a certificate issued by a CA that is not in the browser's list and will be asked if the new CA should be added to the list.

Cross-certification is a solution that could be applied easily, however most of the leading CA companies do not like to provide this service because of the legal implications of cross-certification [20]. This fact causes the various public key infrastructures that currently exist to be incompatible and therefore certificates are not always interoperable across services and countries. There are two reasons for a subject's identity to be impossible to authenticate. First, if the subject certificate is in an untrusted domain due to the absence of trust anchor, and second, because of the use of a new type of SSL certificate, known as lower-assurance SSL certificates. This type of certificate helps provide data confidentiality and integrity, but not authentication of the subject. These certificates are created at reduced cost and with rapid order fulfilment [21]. A deficiency in a subject's authenticity will cause the relying party to incur a higher degree of risk. The following risks could be met [21]:

- A malicious subject could deceive a relying party into believing that the malicious subject's website is operating as part of a known organization whose name is included in the site's SSL certificate.
- A malicious subject could present its website as a specific organization even though no such organization exists.
- A malicious subject could claim to be acting on behalf of an organization to request an SSL certificate.

The Internet provides cheap, easy, and quick access; therefore, it should not be segregated into trusted and untrusted domains. It is important to find an appropriate solution for relying parties to be confident that they can evaluate a subject's trustworthiness. This thesis will try to tackle the issue of authenticating a subject's identity in the presence of an untrusted domain using the trust that is articulated in the subject's CP. The outcomes of this thesis will be a way of making the online environment safer.

1.6 Our Approach

The main contribution of this thesis is defining a process to assist in evaluating the level of trust that can be placed on a subject's certificate in the case that no trust anchor accepted by the relying party can be found. As stated in Section 1.4, certificate

validation involves the construction and processing of a certification path between a trusted anchor and a subject certificate to ensure that all the certificates in the path are valid.

We intend to propose criteria that embody the semantics of the relevant CP to evaluate the subject's trustworthiness. These criteria were developed by considering what makes a good balance between technical and legal requirements, and by the empirical study of several certification authorities. These criteria have been developed in three stages and each stage has been thoroughly tested and analysed in order to evaluate its applicability.

The overall objective of the criteria developed is to provide an extra level of assurance about the subject's certificate in addition to the assurance of the CA that vouches for the identity of the subject to whom it has issued a certificate. The ultimate goal of our approach is to allow the relying party to examine the CP of a subject's certificate, and to try to decide the extent to which the policy of the subject's CA matches with what has been defined in our criteria, and based upon that, the relying party will be able to decide the degree of trust that can put in the subject's certificate.

Our approach to validating a subject's certificate in the absence of a trusted anchor could be interpreted as the construction of a certification path that is a direct path (criteria path) between the subject's certificate CP and the relying party, as shown in the following figure :

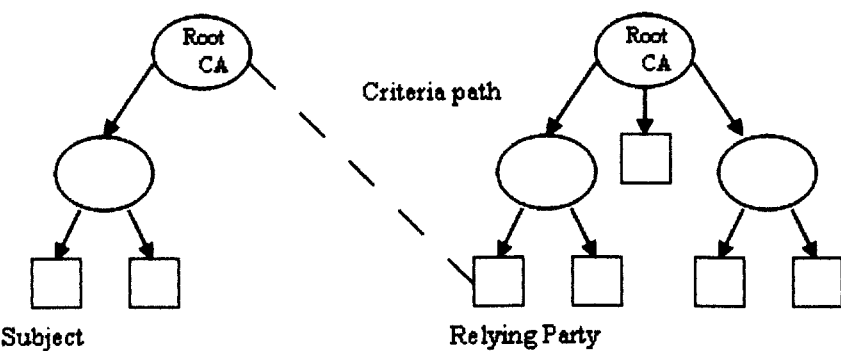


Figure 1-6 Criteria path

A CP, besides creating what we called a domain, is also important when evaluating trustworthiness because it states the obligations of all participants and their liabilities in case of disputes. Cross-certification is based on the degree of trust one domain can place in another, the level of trust is usually what has been written into a CP or a Certification Practices Statement (CPS) [22], see Chapter 3 for more details. Therefore, in our approach we will work with the CP to evaluate the level of trust, making the following important assumption:

We believe that the CP that operates the CP of a subject's certificate which we use to evaluate the level of trust is a genuine CP and is not fabricated.

CPs are written in natural language and so are hard to process automatically. To get round this, we will use the eXtensible Markup Language (XML) language to create a representation for the criteria to ease the process of comparison when evaluating the trustworthiness of participant policies.

1.7 Related Work

The proposed solution uses the CP as a basis for the relying party to decide whether or not to trust the subject's certificate. Our proposed work initially consisted of two concepts: formalisation and comparison. The related work we discuss next also uses the CP to assist comparison.

1.7.1 Formalisation

Klobucar and Jerman-Blazic proposed an approach to formalising a CP in their paper "A formalisation and evaluation of certificate policies" [23] and they selected Abstract Syntax Notation One (ASN.1) as a notation for their formalisation. The elements of the CP are presented in a mixture of their relation to a subject type (CA, RA, end entity), or as a sequence of policy elements according to a corresponding framework. The main characteristics of the formalisation of the policy elements are structural, non-structural, comparable, and non-comparable elements. The ultimate goal of this work was to make CPs easily readable and understandable which could

then help users to evaluate the binding of a public key and a subject's identity and to decide whether to trust the subject's certificate. The formalisation process is mainly a transformation of the contents of CP from natural language to ASN.1 notation. The proposed approach simplifies the presentation of the CP based on a systematic translation from natural language. However, it does not consider the semantic relationships between CP elements and the keywords (such as "MUST", "MUST NOT", etc.) which emphasise requirement levels. Moreover, it also does not handle the constraints relating to the applicability of CP elements.

Bourka et al's ultimate objective of formalising and comparing CPs is different from the previous one. Their target was to facilitate an on-line automated cross-certification service by formalising and comparing CPs [24]. Their method of formalisation depends on extracting a list of possible content values for each CP paragraph to be formalised in XML. This process is combined with assigning weights and scorings for each paragraph in the CP. Weight indicates the importance of the paragraph within the overall CP, and the scorings are assigned to all identified values of each paragraph.

Two different XML document types are produced out by the formalisation of the identified elements of the CP: the Extended CP and the Basic CP. The Extended CP and Basic CP both contain identified content values formalised in XML but the Extended CP also contains the weights and scorings and is considered as a private document which can be used internally for compatibility assessment of external CPs. The Basic CP is publicly published so it can be used for comparison by other organizations. There is no detailed formalisation of their method of specifying the importance of particular CP paragraphs, and there is also no information about the weights and scoring system they used in their formalisation.

1.7.2 Comparison

Comparison in [23] is based on the comparable elements of the formalised CP, e.g. forbidden applications, required minimal length of signature keys, private key protection methods, pieces of identification, or verification methods of private key possession. It uses an order relation value to define the relationship between the CPs being compared. Unfortunately, the proposed approach does not describe the

algorithm which it uses to define the value of the order relation. A partial order rather than a total order results from depending on the comparable elements only.

As we know, the comparable elements do not exemplify the whole CP; therefore, CPs participating in the comparison process should have the same *interest*, meaning that they offer the same or equivalent services. In addition, they must target the same level of applicants (either CAs or end-entities). CPs that differ in interest, will have non-equivalent descriptions in their CP sections. We conclude that the expected result of comparing non-equivalent CPs will not be accurate because of this.

The assessment of compatibility in [24] is accomplished by comparing the Basic CP of the external organization with the Extended CP of the known organization. The assessment is based on the weights and scores set by the known organization in its Extended CP. A mathematical method was developed for CP comparison and it outputs the final result of the compatibility as an integer that results from the addition of weights and scores. As we mention in the preceding section, there is no detailed information about the scoring system used but they do mention that the weights and scoring system are dynamically assigned which means the known organization has control over the specification of its weights and scorings. We think this type of scoring system is suitable when establishing interoperability between organizations (cross-certification) but not for purposes of authentication.

1.8 Thesis Structure

The objective of this thesis is to develop mechanisms to support a comparison mechanism that supports assessment and judgement of a subject's trustworthiness. The thesis consists of 8 chapters and the rest is organized as follows.

Chapter 2 discusses the Public Key Infrastructure more extensively; different standards of PKI are presented with explanations of the basic functions and the components of a PKI system. Certificates are introduced providing an overview of the most common terminologies that relate to them. We discuss certificate validation, presenting the problems that might be encountered when constructing a certification path. The chapter looks at existing proposed solutions for constructing certification

paths, and then describes our approach to constructing the certification path which we called “ATV”.

In Chapter 3, we focus on the background material for implementing our proposed approach; this chapter emphasises the importance of the CP and will explore the obligations that are articulated in a CP for the different PKI elements. We describe the major functions that are necessary through the Life Cycle of a certificate. Also covered are CP issues that relate to security.

Chapter 4 presents the process that has been developed to formalise a CP in XML and shows the different stages that the formalisation went through. In this chapter we define a number of conventions for producing identical formalisations. Each stage of the formalisation has been thoroughly tested and analysed to evaluate its ability to satisfy our needs. The reasons behind needing a new version of the formalisation are shown. Chapter 4 also describes the filtering process that we used to remove unrelated criteria from the first version of the formalism. Finally, we present the final version of our criteria.

Chapter 5 discusses the semantics behind the criteria we have developed. The XML representation for each criterion is also constructed in this chapter. Then we present the numerical evaluation system that has been developed to assign a weight to each criterion. Finally, we explain the comparison results that will come out of the comparison process.

The experimental stage is explained in chapter 6. The criteria are examined against the requirements that are specified in the UNCITRAL law. We conclude that the developed criteria have been defined adequately, and they demonstrate significant potential for estimating a subject’s trustworthiness.

In chapter 7, we study the applicability of the developed criteria. By investigating the developed criteria against a real life cases, we demonstrate the applicability and the coverage. We conclude that the case studies show that the criteria developed handle the correspondence activities that are defined in a real CPs effectively.

Finally, in chapter 8 we conclude by reviewing the work that has been done, and then identifying the directions in which this work can be extended.

CHAPTER 2

SECURING TRANSACTIONS ON THE INTERNET

2.1 Introduction

Enciphering information before it is transmitted over public networks is the only way to build secure communications. An organization can improve its security on the Internet by extending its applications or network security to use public-key encryption for enciphering its information. A PKI provides a comprehensive set of security technologies that meet the needs of business, developers, and users for the secure exchange of information across public networks using private and public keys (Public-key cryptography). In addition to encryption, Public-key cryptography can be used to support authentication, integrity, confidentiality, and non-repudiation. These services allow the establishment of secure communications between two parties without prior contact between them.

This chapter is about understanding PKI. The first step towards this involves knowing the concepts behind PKI. We then present the standards that regulate PKI functions. We follow this by introducing the basic functions and components of a PKI system and then turn our focus to the inside of a PKI architecture to see how connections are established between PKI entities. Repositories and certificates are identified providing an overview of the most common terminologies related to them. The certificate validation procedure is discussed, presenting the problems encountered when constructing the certification path. This chapter looks at five different methods of certificate path construction, and we then propose our approach to constructing the certification path which we call “ATV”.

2.2 Public Key Infrastructure

PKI is, as stated in [15] *“The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Public-Key*

Certificates (PKCs) based on Public-key cryptography". Public-key cryptography fulfils the requirements for securing communications and transaction processing over the Internet. In public-key cryptosystems, each entity holds a pair of related keys, public and private. Anything encrypted with its private key can be decrypted only by its corresponding public key. A PKI is a co-operation between different entities whose ultimate goal is to establish a trust relationship between the parties involved. Services supported by PKI are based on the proper use of public/private key pairs [25]. A PKC is used to verify a digital signature, encrypt data, or both, thus supporting security-related services, including data confidentiality, data integrity, and end-entity authentication. There are several PKI algorithms including, RSA, ElGamal, and DSA, and there are many protocols that use public key techniques, including IPSec, S/MIME, and TLS [26]. These are common industry abbreviations for PKI systems are more concerned with security in establishing keys, which must be kept high to guarantee data integrity.

In order to solve the key management problems of symmetric cryptography, where keys are shared, Diffie and Hellman introduced a new concept in their 1976 paper, "New directions in Cryptography" [27]. They introduced public-key cryptography and claimed that the key management problem was solved; they modified a telephone directory to contain entries with name, number, address and phone number that they called the Public File. Anyone wanting to send an encrypted message should find the recipient's public key first and then encrypt the message with that public key before sending it to the recipient. At the other end, only a recipient who holds the corresponding private key can decrypt the message. In this sense, Public-key (asymmetric) cryptography uses a key pair, the public key which needs to be published openly and a private key which should be kept secret.

The notion of a "digital certificate" was introduced by Kohnfelder in his 1978 MIT bachelor's thesis by digitally signing each name and public key entry of the Public File. The idea was that a certificate is a digitally signed statement binding the key-holder's name to a public key. These certificates could be publicly accessible to anyone who wanted them [11].

The idea of the Diffie and Hellman directory was taken forward by the International Telecommunication Union (ITU) in the 1980s and this work resulted in a standard, known as X.500, which defines all the characteristics of such a directory.

2.3 PKI Standards

Specifications of PKI policies have been clarified in various standards and PKI standardisation has been carried out by a number of different bodies. Currently, there are two open PKI standards: ITU-T Recommendation X.509 V3 and the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) [28]. There are other standards but they either for internal use, such as the National Institute of Standards and Technology (NIST) [29], or where development of the standard has ceased, such as the Simple Public Key Infrastructure (SPKI). X.509 and PKIX are briefly discussed below.

2.3.1 X.509

Recommendation X.509 defines a framework for a Public key Infrastructure (PKI), including PKCs and Certificate Revocation Lists (CRLs) [15]. It defines the data objects that represent these certificates and a framework for attribute certificates which includes definitions of the information objects for the Privilege Management Infrastructure (PMI), attribute certificates and the Attribute Revocation List. X.509 also provides a framework for issuing, managing, using and revoking certificates. Certificate extensions have been defined, and also a scheme for storing the PKI and PMI objects in a directory. Directories play an important role in PKI and make use of PKCs and their attributes. Therefore, X.509 defines the methods for using a directory and for enabling strong authentication. The X.509 standard describes two levels of authentication: simple (using username and password) and strong (using public-key cryptography). When providing secure services, only strong authentication should be used.

2.3.2 PKIX

The PKIX Working Group was established in the fall of 1995 as part of the Internet Engineering Task Force (IETF). The PKIX standard was proposed in [30] as an improvement on X.509, but when this goal was achieved, the PKIX work expanded beyond its original goal and has developed new standards for using X.509 on the Internet. A full list of these standards can be found on the PKIX website: <http://www.ietf.org/html.charters/pkix-charter.html>. PKIX has the same functions as X.509 which supports identification, authentication, access control and authorization functions on the Internet. PKIX also defines a profile for the certificate and CRL protocols. In order to improve interoperability, the PKIX standard applies more restrictions on communicating PKI clients [28]. Because PKIX does not require the use of an X.500 directory system [28], the PKIX uses LDAP attributes integrated with certificates and CRLs for revocation use.

2.4 PKI Services

This section presents those PKI services that provide core security services. The X.509 Recommendation defines PKI functionally as “*The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.*” [15]. Therefore, PKI provides non-repudiation, encryption, authentication, and integrity for electronic business. A PKI is generally considered to be associated with the following services:

2.4.1 Authentication

Authentication is defined in [22] as:

“the verification of an individual's identity and/or the verification of data origin.”

In the PKI this is done by the use of PKCs and digital signature envelopes. Authentication assures the relying party that the authenticating entity is the owner of the private-public key, and this authentication is accomplished when the relying party

uses the authenticating entity's public key to decrypt the message that was digitally signed by the corresponding private key. In fact, the primary goal of authentication in a PKI is to support communication between two parties without any prior contact between them by supporting remote and unambiguous authentication, using PKCs and a trusted CA [31].

2.4.2 Encryption

Public-key cryptography can be used to provide the cryptographic functions for the protection of message confidentiality in a computer network. As we have seen above, key distribution with asymmetric cryptography is easier than with symmetric cryptography [11].

2.4.3 Integrity

Integrity means ensuring the integrity of data end-to-end by preventing unauthorised creation, alteration, or destruction of data during the transaction. PKI assists the recipient who should be able to determine if the message has been altered during transmission.

2.4.4 Non-repudiation

Non-repudiation services ensure that a given action is undeniable; repudiation occurs when an individual denies involvement in a prior transaction (i.e. agreements and procedures). Thus, non-repudiation means that an individual cannot successfully deny involvement in a legitimate transaction. The most basic requirement for non-repudiation is that a private key owner must be the only person in control of it, and that it should be stored securely [15].

2.5 PKI Architecture

Architecture is defined as “*the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time*” [32]. In this

section, we aim give more details about the relationship between the different entities of a PKI, especially the relationship between the CA and the end-entities. Different logical architectures have been formed based on the interrelation between these, and CP and CPS basically play a role in governing all the behaviours in these different architectures. PKI architectures are of three different types:

2.5.1 Hierarchical Architecture

A hierarchical architecture consists of a top level “root” CA that issues certificates to subordinate CAs. These CAs certify their descendants who are either CAs below them in the hierarchy, or to end-entities, and so on. Every entity in the community holds a copy of the public key of the root CA [33]. All end-entities base their trust on the public key of the “root” CA which is the trust anchor, and this principle enables end-entities to validate any certificate by verifying the certification path of certificates from the trust anchor CA. For example, Alice verifies Bob’s certificate, issued by CA 4, then CA 4’s certificate, issued by CA 2, and then CA 2’s certificate issued by CA 1, the root, whose public key Alice knows. Figure 2-1 illustrates this example.

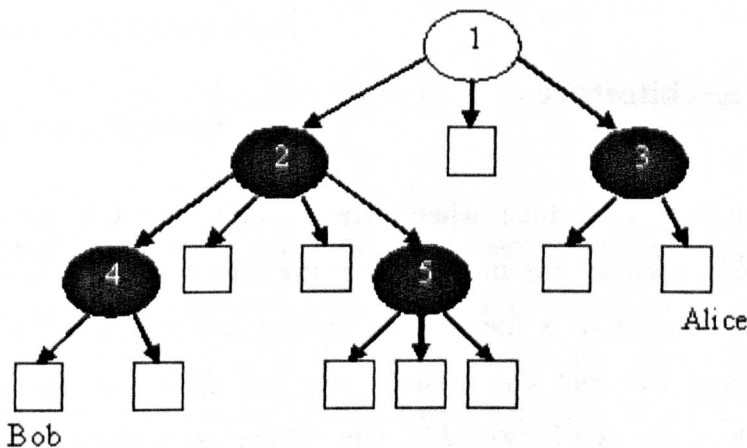


Figure 2-1 Hierarchical Architecture

2.5.2 Mesh Architecture

In a mesh architecture there is no single root CA but more than one root CAs and each CA issues certificates to the others (cross certification) [33]. The relying party bases path validations on the public key of a nearby CA, as a trust anchor, generally the one

that issues his/her certificate because the relying party knows the public key of that trusted CA. So, for example, Alice knows the public key of CA 3, while Bob knows the public key of CA 4. There are several certification paths that lead from Bob to Alice. The shortest requires Alice to verify Bob's certificate, issued by CA 4, then CA 4's certificate issued by CA 2 and finally CA 2's certificate, issued by CA 3. CA 3 is Alice's CA and she knows the public key of trust anchor CA 3. Figure 2-2 explains mesh architecture.

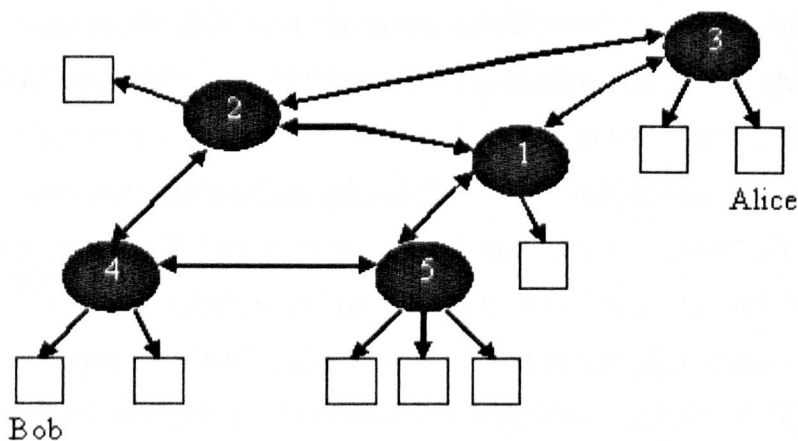


Figure 2-2 Mesh Architecture

2.5.3 Single Architecture

A single architecture is formed when there is only one CA providing all the certificates for end-entities. This architecture is the most basic and the simplest model for a PKI. It is similar to a hierarchical architecture where every entity in the community obtains the root CA's public key but differs in the sense that the maximum depth of the tree is two [34]. The relying party needs only to check the revocation status of any certificate to validate it. Figure 2-3 shows a single architecture system.

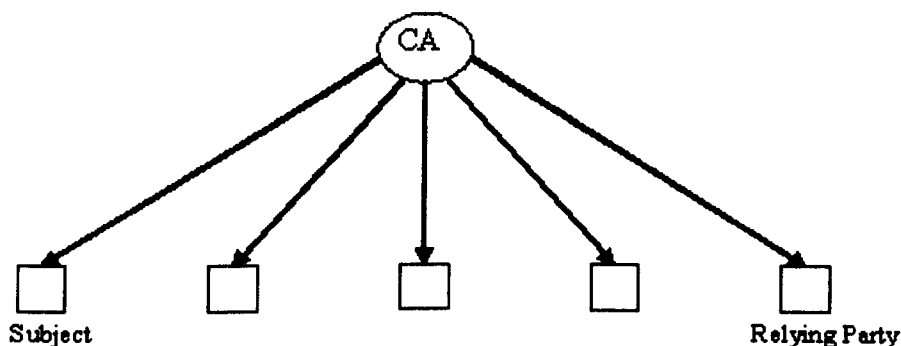


Figure 2-3 Single Architecture

2.6 Connecting Architectures

In the previous section we discussed different architectures from which PKI can be logically formed based on the relationship that exists between trust anchors and relying parties where the relationship is managed by the same CP. Increasingly, PKI can be implemented in a distributed fashion: instead of using a single CA architecture, it could join with other architectures that operate different CPs allowing end-entities to use a CA based on their particular needs. In this section we emphasize the bindings that exist between PKI architectures.

2.6.1 Cross-certification

Cross-certification is the act of providing a CA with a certificate signed by another CA in another hierarchy. The cross domains agree to trust and rely upon each other's PKCs, keys and policies in order that each domain can vouch for each other's certificates which results in extending the trust relationship of a CA. A certificate in cross-certification is called a cross-certificate. The subject of the certificate is called the subject certification authority. The issuer of the cross-certificate is called an intermediate certification authority [15].

2.6.2 Bridge CA

Bridge CAs do not cross-certify each other. In addition, Bridge CAs are not intended to be used as trust points by the users of the PKI, unlike intermediate CAs in Cross-

certification; instead, a Bridge CA acts as a mediator, that it introduces one organization to another. Each root CA enters cross-certification with the Bridge CA whose job is to facilitate the communication under one or more certificate policies [11].

2.7 PKI Components

As stated previously, a PKI is a framework of people, processes, policies, protocols, hardware, and software used to generate, manage, store, deploy, and revoke PKCs. In the following we discuss these components further:

2.7.1 Certification Authority

The CA plays a critical role because it is the primary component of a PKI. According to the ITU-T Recommendation X.509, a CA is “*an authority trusted by one or more users to create and assign public-key certificates.*” [15]. The main task of a CA is to confirm the identity of an end entity. The process begins with an entity providing the CA with sufficient proof of his/her identity. After satisfactory verification of the identity credentials supplied, the CA generates a public-private key pair for the entity, and creates a certificate for the generated public key which it cryptographically signs. The policies and procedures the CA has established to confirm the user’s identity will decide the level of acceptance that other entities have of that CA [31].

The CA must distribute its public keys to all entities that trust the CA’s certificates. The PKI will generally have a root CA, which is at the top of the CA hierarchy and has no superior CA to vouch for it. This CA issues certificates to other CAs and its public keys are distributed as self-signed certificates. The CA’s daily tasks are to issue, maintain, verify, and revoke certificates. A CA operates under a policy known as a CP and functions operationally according to a CPS. The CP and CPS are discussed in Chapter 3.

2.7.2 Registration Authority

The RA does not itself issue certificates and is an optional but common component of a PKI. The primary purpose of an RA is to register and verify an end entity's identity, with a valid photo-id and/or valid official documents, and to determine if an end-entity is entitled to have a CA issue a PKC [31]. An RA must make sure that all procedures and processes are followed properly as defined in the CA's CP and CPS.

2.7.3 End-entity (Subscriber)

An end-entity or subscriber is defined in the Internet Certificate and CRL Profile as a *"user of PKI certificates and/or end user system that is the subject of a certificate"*. End-entities use certificates to identify themselves and must be able to generate a public/private key pair and securely store and use the private key [31].

Starting in Chapter 4 we will use "subject" to refer to end-entities; we prefer this term as it complies with the authentication process that is performed on an end entity's identity.

2.7.4 Relying Party

Defined in [20] as *"The entity that uses certificates and Certificate Revocation Lists in order to rely on the digital signature of the sender of a signed message, or the public key"*.

2.7.5 Repository

The majority of PKI vendors use repositories for storing and retrieving certificates [25]. The term repository is defined in [20] as *"An online system maintained by a CA for storing and retrieving certificates and CRL"*. Publishing and distributing valid certificates and the CRL is one of the duties of a CA. Each CA has one or more Certificate/CRL Repositories used to distribute certificates and CRLs using common protocols such as LDAP, HTTP and FTP [20]. We will look at the two main forms of repository: certificate and CRL repositories.

2.7.5.1 Certificate Repository

The Internet is the largest distributed system; and therefore, to integrate certificate services with Internet users, certificates should be available to all system users on the Internet. For this reason, the idea of distributed repositories (directory) had been introduced and certificate repositories store all the certificates ever issued by a CA.

X.500 is a standard for directory services issued by the International Union (ITU). It specifies both the structure of the directory information and of the protocols needed to access the information [35]. X.500 also provides a specification for a distributed directory based on hierarchically named information objects (directory entries) [35]. Each entry belongs to one or more object class (e.g. country, person, organization). Each entity contains a set of attributes which holds the object information, and at least one attribute's value specifies a name for an entry [20]. This name is known as a distinguished name (DN) which is a unique identification. X.500 supports replication, access control and search mechanisms.

The Lightweight Directory Access Protocol (LDAP) was designed to simplify access to X.500 and to make the directory available to all clients (machines and applications) [20]. LDAP is subset of X.500, but LDAP goes beyond the original purpose and attempts to position itself as the only directory protocol required, and hence implies that the full X.500 protocols are unnecessary [35]. Using LDAP with X.500 is inefficient; the reason being the heavyweight nature of X.500. A site, holding only local data, has to bring up a full X.500 service before the user can use LDAP to access these data. A new protocol has been developed called “slapd”, a stand-alone LDAP server which has its own local database [20]. X.509 tries to simplify the use of a directory by defining specific directory attributes for storing the certificates of the CA and end-entities. All the directory attributes are listed in the table 2-1 with their definitions as specified in [15]:

Directory Attributes	Function
User certificate attribute	A user could have more than one public-key certificate from one or more CAs. The userCertificate attribute type contains the public-key certificates a user has.
CA certificate attribute	<p>A CA stores its self-issued certificates and certificates issued to this CA by other CAs in the same realm as this CA in the cACertificate attribute of a CA's directory entry.</p> <p>In the case of v3 certificates, a basicConstraints extension with the cA value set to TRUE should be included in these certificates (see section 2.7.6.1).</p>
Cross certificate pair attribute	<p>Any certificates issued to this CA by other CAs should be stored in the issuedToThisCA elements of the crossCertificatePair attribute of a CA's directory entry. Optionally, any certificates issued by this CA to other CAs can be contained in the issuedByThisCA elements of the crossCertificatePair attribute. The certificate issuer shall store a certificate in the issuedByThisCA element of the crossCertificatePair attribute of its own directory entry if the certificate has been issued to a subject CA which is not a subordinate in a hierarchy. If a single attribute value contains both the issuedToThisCA and the issuedByThisCA, the issuer name in one certificate shall match the subject name in the other and vice versa.</p> <p>In the case of v3 certificates, a basicConstraints extension with the cA value set to TRUE should be included in these certificates (see section 2.7.6.1).</p>
Certificate revocation list attribute	A list of revoked certificates will be contained in this attributed.
Authority revocation list attribute	This attribute contains a list of revoked authority certificates.
Delta revocation list attribute	This attribute type will contain a delta CRL in a directory entry.
Supported algorithms attribute	In the case that there is communication with a remote entity using certificates as defined in this Directory Specification, this attribute will support the selection of an algorithm to be used in this communication.
Certification practice statement attribute	The certificationPracticeStmt attribute will hold information about an authority's certification practice statement.
Certificate policy attribute	The certificatePolicy attribute holds information about a certificate policy.
PKI path attribute	The PKI path attribute contains certification paths, each consisting of a sequence of cross-certificates.

Table 2-1 Directory Attributes

A Note Regarding Directory Attributes

The directory attributes are defined to play an important role in simplifying access to stored certificates and to help in performing the verification process which in turn

supports the certification process. However, [25] includes a number of notes about the directory attributes and their usefulness for finding the right certificate.

First, it is expected that the CA should make the `cACertificate` attribute available for its own directory with its self-signed certificates as well as certificates issued by the CA in support of CA key update.

Second, they may see the same certificates issued to a CA by other CAs in the same realm stored in the `cACertificate` attribute of its own directory entry. The realm is undefined and subject to interpretation, an example of this is a single PKI domain consisting of a hierarchy of CAs. The subordinate CAs will store the certificates issued to them by their superior CA in the `cACertificate` attribute of their own directory entry. However, we cannot be certain that all vendors will implement this consistently.

Third, they would expect that certificates issued to this CA by other CAs contain the `issuedToThisCA` elements of the cross-certificate pair. Consequently, both `cACertificate` and `issuedToThisCA` may be populated when the issuing CA is in the same realm as the CA to which it was issued.

Finally, in the case when a CA issues certificates to other CAs that do not belong to the same hierarchy, they expect the `issuedByThisCA` attribute to be populated in the issued certificates. They also expect to see certificates containing `issuedByThisCA` issued to peer CAs in a distributed trust model. They note that we should not expect that `issuedByThisCA` is always populated in a hierarchical domain.

[25] describes more expectations but as mandatory behaviour for CAs who conforms to the 4th edition of X.509:

1. The `cACertificate` attribute of the issuing CA's directory entry should store all self-issued certificates.
2. The `issuedToThisCA` element of the cross-certificate pair attribute of the CA's directory entry should store all certificates issued to a CA except for self-issued certificates.

3. The issuedByThisCA element of the cross-certificate pair attribute of the issuing CA's directory entry should store all certificates issued by a CA to a non-subordinate or peer CA.

[25] also states that although the pkiPath attribute has been defined to store partial or complete certification paths in the 4th Edition of X.509:

This attribute can be stored in the CA directory entry and would contain some certification paths from that CA to other CAs. This attribute, if used, enables more efficient retrieval of cross-certificates that form frequently used certification paths. As such there are no specific requirements for this attribute to be used and the set of values that are stored in the attribute will likely not represent the complete set of forward certification paths for any given CA.

But they state that there are no existing implementations that use the pkiPath attribute as so described. The reason for not using this attribute could be that it is optional.

2.7.5.2 Certificate Revocation List Repository

A CRL is a list of certificates, created by a CA, that have been revoked before their scheduled expiration date. CRLs have to be digitally signed by CAs or, in general, by CRL issuers which provides for the integrity and authenticity of the CRL [36]. A certificate-using application can use the most recent CRL to check whether or not a subject's certificate has been revoked for any reason. In 1988, version 1 (v1) of the CRL was defined in the original X.509 specification. Unfortunately, a number of drawbacks existed in v1, including [36]:

- The CRL size could easily grow beyond acceptable limits.
- Functionality limitations.
- The system was subject to CRL substitution attacks (maliciously substituting one with another without detection).

These problems were solved by Version 2 (v2) CRLs by introducing the notion of extensions, much the same as the introduction of extensions to Version 3 X.509 PKCs.

CRLs classify revoked certificates by their certificate serial numbers. In addition to the serial number for the revoked certifications, the CRL also contains the reason for revocation for each certificate and the time the certificate was revoked. CRL issuance is performed periodically on a rotational basis of hourly, daily, or weekly [37]. At every CRL update, new entries are added and they must not be removed from the CRL until the revoked certificate expires [37]. Complete CRLs are suitable for small CA domains particularly those in which the number of end-entities is relatively small, but criticisms have been raised with respect to complete CRLs in CA domains with large number of entities, and these are [36]:

1. The issue of scalability: given that revocation information must remain for the life of a certificate, therefore, CRLs grow as time goes by and complete CRLs can become large in some domains; which means that more and more data must be searched and downloaded.
2. The timeliness of the posted certificate revocation information: as a result of the inflated size of the CRLs, the download time will be large each time a certificate is validated.

Various mechanisms are employed to split the CRLs into multiple lists which enhance performance and capacity [20]. In the following we present these mechanisms along with other relevant information:

Certification Authority Revocation Lists

CAs issue Certification Authority Revocation Lists (CARLs) exclusively to contain the CAs revoked certificates. As its name implies, it is a CRL devoted exclusively to revocation information associated with CAs. Thus, by definition, CARLs do not contain end-user certificate revocation information. The issuer of a CARL is either a superior CA (who revokes any subordinate CAs) or a CA engaged in cross-certification (who revokes a cross-certificate that it has issued) [36].

End-entity Public-key Certificate Revocation Lists

An End-entity Public-key Certificate Revocation Lists (EPRL) is the opposite of the CARL, and it contains certificates issued only to end-entities. Thus, by definition, revocation information for CAs is not included in EPRLs [36].

CRL Distribution Points

CRL Distribution Points, also known as partitioned CRLs, allow revocation information within a single CA domain to be stored in distributed CRLs. This scheme gives CRL Distribution Points two significant benefits over complete CRLs:

1. CRLs are partitioned into more manageable pieces to avoid the proliferation of large CRLs.
2. A relying party will be directed automatically to the location of the CRL Distribution Point because certificates can point there.

The CRL Distribution Point offers a more scalable method of implementing a CRL as compared to complete CRL postings; however, there are criticisms: that CRL Distribution Points are static and cannot handle change when the organization or CA changes, moreover, the issuing CA must have prior knowledge of the partitioning structure [36]. A dynamic partitioning scheme is discussed next.

Redirect CRLs

Redirect CRLs were developed to overcome the drawbacks associated with the use of CRL Distribution Points by allowing the CRL partition sizes and storage locations to vary over time. Flexibility in CRLs can be accomplished by creating a dynamic CRL partition based on a number of elements, including certificate serial number ranges, revocation reasons, certificate types, name subtrees, or any other range criteria that might apply to CRL information, and CRL partitioning also assists redirection of CRL inquiries. The IETF PKIX working group introduced the notion of dynamic partitioning in the 2000 version of X.509 [X509-00] through the definition of the CRL Scope and Status Referral extensions [36].

The Redirect CRL uses a X.509 Version 3 Certificate extension, the CRL Distribution Point Extension, and a X.509 Version 2 CRL extension, the Redirect Pointer, to redirect a relying party to the appropriate CRL. This intermediate CRL is referred to as a Redirect CRL. The Certificate CRL Distribution Point Extension points to a Redirect CRL which contains an X.509 Version 2 CRL with a valid Status Referral extension. The Status Referral Extension in turn points to the correct, and possibly dynamic, CRL partition.

Delta CRLs

Publishing complete (base) CRLs more frequently has positive and negative consequences. Making relying parties aware of any revoked certificates instantly is a positive consequence, however, this results in a negative outcome by increasing the size of the base CRLs. This negative outcome leads to the following implications [34]:

1. Increased network traffic due to the more frequent downloading of the updated CRL.
2. Delaying relying parties who connect over slow connections due to the long download time caused by the size of the updated CRLs.

The solution proposed is to use delta CRLs. The size of a delta CRL is much smaller than a base CRL which means publishing delta CRLs frequently meets the requirements of relying parties for timeliness and freshness of certificate revocation information. Delta CRLs, defined in RFC 2459, address the problems of publishing a base CRL frequently, by publishing changes to a base CRL in a smaller file known as a delta CRL. With delta CRLs, a relying party can download a base CRL at longer intervals, and then download smaller delta CRLs at shorter intervals to validate any certificates presented. Publishing delta CRLs at short intervals, such as once an hour, increases the confidence in the certificates being validated [34].

Indirect CRLs

The Indirect CRL mechanism assists multiple CAs in publishing revocation information in a single CRL and a relying party is therefore able to avoid the retrieval of revocation information from multiple CRLs being issued by multiple CAs [36].

2.7.6 X.509 Version 3 Certificate

The Internet Certificate and CRL Profile [37] defines certificates as “*data structures that bind public key values to subjects*”. Certificates afford confidence by offering a binding to public key users which helps them ensure that the associated private key is owned by the correct unknown subject (person or system) with which an encryption or digital signature mechanism will be used. Moreover, a trusted CA digitally signs each certificate (binding) which also increases the confidence in the subject’s certificate.

Digital certificates in this sense act as an electronic identification used to verify the identities of communicating parties in on-line transactions. The certificate is a form of a credential such as driving license, birth certificate, or passport. In a face-to-face transaction, the signature is one of these credentials when compared to the signature sample and the face of the person compared to the picture on the credential to ensure that it truly belonged to the person providing the signature and the face. The digital certificate would be used to perform these functions in the case of an electronic transaction [38].

The first standard issued which defined certificate formats was in 1988, ITU-T X.509 (formerly CCITT X.509) or ISO/IEC 9594-8, and it is called the version 1 (v1) format [37]. V1 was developed as part of the development of the X.500 Directory recommendations. In 1993 X.500 was revised which result in two more fields being added to v1 to produce version 2 (v2) format.

The deployment process of the Privacy Enhancement for Internet Electronic Mail [RFC 1422] has shown that there were deficiencies in v1 and v2 in several respects and that improvements to these formats needed to be carried out [37]. In 1998 a new standard was proposed by ISO/IEC, ITU-T and ANSI X9 to meet these new

requirements called the X.509 version 3 (v3) certificate format which extends the v2 format by adding extension fields [37]. This version became popular because it was used by most enterprise and government deployments, moreover, the version 3 certificate extensions also helped in controlling business relationships within and across PKI domains [25].

2.7.6.1 Types of Certificates

There are two major types of digital certificates: CA certificates and end-entity certificates [15]. Certificates issued to CAs are known as CA certificates, and certificates issued to end-entities are referred to as end-entity certificates. In the certificate there is an extension called Basic Constraints (basicConstraints) which helps to differentiate between CA certificates and end-entity certificates [25]. The following further explains these types:

CA Certificates

CA certificates can be classified into three different types:

1. Cross-certificates are CA certificates in which the issuer and subject are different entities. Cross-certificates are used to establish trust relationship between the two CAs [15].
2. Self-issued certificates are CA certificates in which the CA issues the CA certificate to itself. Self-issued certificates are generated to support changes in policy or during a key rollover operation [15].
3. Self-signed certificates are CA certificates that are used to validate all certificates issued by that CA and the digital signature may be verified by the public key bound into the certificate [15].

End-entity Certificates

End entity certificates are used to verify the identity of a specific entity which is not authorized to issue certificates, these certificates are known as end-entity certificates, identity certificates, or personal certificates [39].

2.7.6.2 Certificate Fields

A certificate binds the public key to the owner's identity, and consists of three required fields [20]:

1. **tbsCertificate**

This field contains information about the subject such as the subject name, or the subject's public key. It also includes the certificate issuer name, a validity period, a version number, a serial number, and unique identifier fields. It also usually includes extensions [37].

2. **Signature Algorithm**

The signature algorithm field identifies the cryptographic algorithm used by the CA to sign the subject certificate [37].

3. **Signature Value**

This field contains the CA's digital signature. The signature means that the CA certifies the validity of the information in the tbsCertificate field [37].

The basic certificate fields of a v3 certificate are the same as that of a v2 certificate apart from the new extensions field. Figure 2-4 shows all fields and a description of each field of the X.509 v3 certificate basic follows.

Certificate Version
Certificate Serial Number
Signature Algorithm Identifier
Issuer X.500 Name
Validity Period
Subject X.500 Name
Subject Public Key Information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Issuer Digital Signature

Figure 2-4 X.509 Certificate Format

Version

An indicator of the X.509 certificate version number, it can be 1, 2, or 3. If extensions are omitted, the version of the certificate should be 1. If extensions are used, the version must be 3. If either the issuerUniqueIdentifier or subjectUniqueIdentifier fields are present with the absence of extensions fields, the version must be version 2.

Serial Number

The certificate serial number is a unique numerical identifier for each certificate assigned by the CA.

Signature

This field contains the identifier of the digital signature algorithm used to calculate the digital signature on the certificate.

Issuer Name

The issuer name identifies the entity that has signed and issued the certificate. The syntax of the issuer name is an X.500 distinguished name (DN).

Validity

This field defines the validity period of the certificate as dates and times for the start date and the expiry date by using the elements notBefore and notAfter. The validity period is given in universal time encoding (UTC) or Greenwich Mean Time (GMT) [37].

Subject Name

This field identifies the entity holding the private key corresponding to the public key identified in the certificate. Subject name is specified in the X.500 DN. The subject name can be found in the subject field and/or the subject alternative name extension. If the subject name is present only in the subject alternative name extension, then the

subject name must be an empty sequence and the subject alternative name extension must be present [37].

Subject Public Key Information

Subject Public Key Information: specifies the value of the public key owned by the subject, and specifies an algorithm identifier specifying both the public key algorithm and the hashing function with which the public key is to be used.

Unique Identifiers

The issuer and subject unique identifier are used to offer the possibility of reuse of subject and/or issuer names over time. The Internet Certificate and CRL Profile recommend that names not be reused for different entities and that Internet certificates not make use of unique identifiers. Furthermore CAs conforming to the Internet Certificate and CRL Profile should not generate certificates with unique identifiers.

2.7.6.3 Certificate Extensions

As we have seen, extensions were first introduced in the X.509 v3 standard and they provide methods for associating additional fields with the certificate [37]. Certificate extensions provide a means of expanding the original X.509 certificate information standards with any number of additional fields. The X.509 v3 certificate extensions assist in defining restrictions on certificate applicability, alternative subjects, and they can carry information unique to special communities.

Each certificate extension is marked either critical or non-critical. If an extension is marked as being non-critical, it means that if an application does not recognize or understand the extension it can be ignored by the application and the certificate can still be used. An application or system must reject a certificate with an extension marked as critical if the application does not recognize the extension.

Each extension consists of three fields: Type, Value and Criticality.

- Type: contains an object identifier (e.g. text string, date ...etc).

- Value: contains the actual data for the extension.
- Criticality: a bit flag that indicates if an associated extension value is critical or non-critical.

Tables 2-2 and 2-3 show the two recommended types of extensions, standard extensions and private Internet extensions as specified in [37]:

STANDARD EXTENSIONS	Extension Name	Function	Criticality
	Authority Key Identifier	The authority key identifier extension is an extension for identifying the certificate authority's public key corresponding to the private key used to sign the certificate.	Non-critical
	Subject Key Identifier	The subject key identifier extension is an extension for identifying the subject's certificate that contains a particular public key.	Non-critical
	Key Usage	The key usage extension specifies the purposes for which a certificate can be used. (e.g., encipherment, signature, certificate signing).	Critical
	Private Key Usage Period	The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate.	Non-critical
	Certificate Policies	The certificate policies defines one or more policies under which the certificate has been issued and the purposes for which the certificate may be used, defined by a sequence of policy information terms, each consisting of an object identifier (OID) and optional qualifiers.	Either
	Policy Mappings	The policy mappings extension is used in CA certificates only. It lists one or more pairs of OIDs used to indicate that certain policies in its own domain can be considered equivalent to some other policies in the subject certification authority's domain.	Non-critical
	Subject Alternative Name	The subject alternative name extension is for allowing the binding of additional identities to the subject of the certificate. It may be used in addition to the certificate's subject name or as a replacement for it. Defined name forms include Internet electronic mail address, DNS name, IP address, and uniform resource identifier (URI).	Either
	Issuer Alternative Names	The issuer alternative name extension is used to associate Internet style identities with the issuer of the certificate. Defined options include Internet electronic mail address, a DNS name, an IP address, and an URI.	Non-critical
	Subject Directory Attributes	The subject directory extension is used to include additional attributes (e.g., nationality) for identifying the subject of a certificate	Non-critical
	Basic Constraints	The basic constraints extension is used to identify whether the subject of the certificate is a CA and how deep a certification path may exist through that CA.	Critical
	Name Constraints	The name constraints extension is used to indicate a name space within which all subject names in subsequent certificates in a certification path must be locate.	Critical

	Policy Constraints	The policy constraints extension is used to restraint path validation in two ways. It can be used to indicate required acceptable policy identifiers that each certificate in a path contain and/or prohibited policy mappings.	Either
	Extended Key Usage	The extended key usage is a restriction method and indicates one or more purposes for which a certificate can be used. These purposes may be in addition to or in place of the basic purposes indicated in the key usage extension.	Either
	CRL Distribution Points	The CRL distribution points extension indicates the location of the CRL partition where revocation information associated with this certificate resides.	Non-critical ..
	Inhibit Any-Policy	The inhibit any-policy indicates that the special any-policy OID, with the value 2 5 29 32 0, should not be considered a legitimate match for other policy identifiers.	Critical
	Freshest CRL	The freshest CRL extension provides a pointer to the "freshest" delta CRL information. The freshest CRL extension is placed in the full CRL to indicate where to find latest delta CRL.	Non-critical

Table 2-2 Standard Extensions

PRIVATE INTERNET EXTENSIONS	Extension Name	Function	Criticality
	Authority Information Access	The authority information access extension indicates how information or services offered by the issuer of the certificate can be obtained.	Non-critical
	Subject Information Access	The subject information access extension indicates how information and services for the subject of the certificate in which the extension appears are accessed	Non-critical

Table 2-3 Private Internet Extensions

2.8 Certificate Issuance

A CA issues a certificate to another CA or to an end-entity (e.g., end-users, devices, Web servers, processes) [25]. The following steps illustrate how the CA creates a certificate:

1. An applicant needs first of all to have a key pair (public and private), that could be generated in one of the following ways:

- By using a public key algorithm, an applicant creates a public-private key pair, and then encrypts the private key and keeps it locally [40]. Here, the applicant needs to send its public key to a CA.
- By using a third party which must release the private key in a secure way to the applicant and destroy the keys and all information that relates to the key pair [15].
- By the issuer of the certificate, who is trusted by the applicant [15].

Afterwards the applicant submits a certificate request to an RA with appropriate identity information, such as their name, address, telephone number and e-mail address.

2. In accordance with the Certificate Practice Statement (CPS), the RA will validate the identity information in order to make sure it belongs to the applicant. The RA does this by checking mail, making phone calls, asking for identification, etc. According to the results of this identity verification, the RA may approve or reject the request.
3. If the request is approved, the RA directs it to the CA to issue a certificate for the applicant.
4. The CA generates a certificate and signs it with its private key.
5. The RA sends a notification, containing the serial number of the certificate, to the applicant, and then the applicant retrieves the certificate from a repository by presenting the certificate's serial number to the RA Operator [29].

2.9 Certificate Revocation

A certificate is issued with the expectation that it is used through its lifetime, which is defined by the start and expiry date of its validity period. For example, a certificate's validity period may be one day, thirty years, or even longer. Once a certificate is issued, it becomes valid when its validity time has been reached until the certificate

reaches its expiration data. Unfortunately, there are various circumstances that invalidate a certificate prior to its expiration date [37]. Such circumstances include:

- The certificate is no longer used.
- The CA had issued a certificate improperly.
- Failure of the subject to adhere to policy.
- The details of the certificate have changed. For example the subject's name or the subject's association with CA (when an employee terminates employment with an organization).
- The private key has been lost or exposed, or there is suspicion that the private key has been lost or compromised.

Under such circumstances, the CA needs to revoke the certificate and enter it on a CRL.

2.10 The Certificate Validation Process

A certificate is a proof of identity on the Internet, so the user can claim that his public key is reliable, and a CA can vouch for the identity of the user. If there is another party (Bob) who wants to communicate with a user (Alice), Bob will ask Alice to show him her certificate. Bob will trust Alice's certificate if he trusts its issuer and Bob will start communicating with Alice. Alternatively, if Bob does not trust the issuer of Alice's certificate, then Bob needs to get the public key of the CA that issued Alice's certificate. Bob starts to extract information from Alice's certificate, uses it to verify the other certificate, and Bob continues this process till he finds a trusted CA. This type of validation is called certification path processing.

The certificate validation process consists of constructing a certificate path between a trust anchor and a subject. The process of constructing consists of [25]:

- Path construction: constructing one or more candidate paths.
- Path validation: checking that all certificates on the path are valid and they satisfy any constraints required for validation.

The 4th Edition of X.509 and the Internet Certificate and Certificate Revocation List Profile as defined in RFC3280 offers the latest guidelines for implementing certification path validation. Despite the importance of the validation process there is little published research into it. Neither [15] nor [37] say anything about the process of constructing certification paths [25].

[25] states that building a certification path is a complex process based on trial and error, moreover, there is a lack of standardization or harmonization of methods for carrying it out.

2.10.1 Evaluating Certification Paths During Path Construction

The evaluation process has to be executed concurrently with the path construction process especially in a complex, richly interconnected PKI environment otherwise we will face problems which can lead to inefficiencies [25]. It is possible to apply certain constraints in order to submit the best candidate certification to the path validation logic to produce an acceptable path [25]. There are several criteria which could be used during path construction which will assist in eliminating paths that would not help in building the target certification path. We will achieve a good result when more than one of the constraints can be used during the process of constructing the certification path. These constraints are name and certificate policy constraints.

2.10.2 Direction of Path Construction

Generally, certificates are stored in directories which help the process of building, constructing, discovering or developing the certification path connecting the trust anchor and the subject. The build direction of the certification path is consequent on the certificates' location in the directories [26]. There are two directions for constructing a certification path, forwards (from subject to trust anchor) and backwards (from trust anchor to subject).

2.10.2.1 Forward versus Backwards

As stated in [25] the forward way of working with a strict hierarchy is efficient because we are always guaranteed to find certificates that have been issued to each

subordinate CA contain in the issuedToThisCA element of the cross-certificate pair attribute. In addition, in the case of the strict hierarchy we always end up with a limited number of possible certification paths and sometimes with only one, if a CA has only one certificate.

In the case of a distributed environment, the reverse direction will be more efficient for constructing a path, because we may encounter tens or even hundreds of forward elements associated with a given CA, not just one or two. The cross-certificate pair attribute element, issuedToThisCA, will not help here and will divert us from the path we are seeking because we could encounter a large number of CAs who issued certificates to this CA. Therefore working with the issuedByThisCA element of the cross-certificate pair attribute will help in constructing a (partial) path starting from the relying part's trust anchor since we are answering the question "to whom have you issued certificates" [25].

2.10.3 Problems with Certification Path Construction

2.10.3.1 Loops

The 4th edition of X.509 states that each certificate in a certification path must be unique and also declares that a certificate should not appear more than once in any value of a certificate's attribute. We can apply the previous rule during the path creation process by keeping track of all certificates that have been validated and if any name appears twice, we can backtrack as necessary [25]. If the tracking is based on checking the subject's DN, we could have duplicates because there is more than one public key with the same DN. Thus, we need a tracking system that avoids a certificate that appears more than once in the constructed certification path. This can be accomplished through direct certificate comparison [25].

2.10.3.2 More Than One Branch Leads to the Candidate Path

We could end up with more than one candidate path linking the trusted anchor and the subject certificate where they meet all of the certification path criteria equally. This happens in the absence of any other criteria to prioritize one path over another.

Therefore, it will be better to submit the shortest path rather than the longest one to the path validation logic [25].

2.10.4 Related work in Validating Certificate

X.509 and the Certificate and Certificate Revocation List profile are silent when it comes to the process of path construction; consequently, a proposal for finding a method for building certification paths becomes necessary. A few proposed solutions have been made for finding an algorithm for constructing certification paths:

Five proposals for validating a certificate follow:

1. Certificate chains
2. Hierarchy graphs
3. Certification path validation service
4. Modified LDAP server
5. Dynamic path determination

Finally, we demonstrate our method for validating the certificate which is called "Ants traversal and validation".

2.10.4.1 Certificate Chains

A certificate chain is described in [28] as a structure that contains all the certificates, from the CA immediately below the root CA to the user, signed and wrapped by the root CA of the hierarchy. The client stores all self-signed root CA certificates that are needed to authenticate subjects of different hierarchies. Path processing with certificate chains is easy, because the determination process is performed at the time of certificate-chain signing and wrapping, therefore, only the validation mechanism needs to be applied.

2.10.4.2 Hierarchy Graphs

This method, discussed in [28], is a program that resides on the client computer which checks and stores all the local CA hierarchy to which its user belongs before path

construction begins. The hierarchy is a directed graph where the nodes represent CAs and the arcs are the certificates that interconnect these CAs. Nodes are inserted into the graph after the CA's integrity has been checked, starting with the CA who issued the target certificate and the insertion process continues until a node intersecting with the local hierarchy graph is found. After the determination task ends, path validation is performed. The proposed algorithm is designed to find the shortest path among multiple alternative paths.

2.10.4.3 Certification Path Validation Service

In [28], it is suggested that a Data Certification Server (DCS) could be responsible for path processing with the DCS doing this by validating signatures and providing updated certificate status information. For authentication, the client sends an authentication request to the DCS, together with the subject certificate. The DCS will do validation for the subject's certificate by retrieving all necessary certificates from the distributed repositories. The DCS will determine and validate the path and send a token to the client. This token will allow several transactions for a limited time, without requiring the authentication process to be repeated. It is clear that the client implementation would be simple because all processing is performed by the DCS.

2.10.4.4 Modified LDAP Server

A repository access server is described in [28] which will determine the path after it receives a request from a client. It then sends the path to the client including all the component certificates. The client is responsible for validating the received path. The LDAP protocol is used for accessing the repository.

2.10.4.5 Dynamic Path Determination

Dynamic path determination, as described in [28], allows a root CA only to issue cross-certificates to the root CAs of other hierarchies and no trust is to be transferred between such root CAs; and therefore, only one certification path is possible. The path is constructed by retrieving each certificate from a repository via LDAP, and a local list, called a local trust chain, is stored in the client environment. The local list

will assist in the process of certification path verification. It contains all the certificates that make up the path between the user's issuing CA and its hierarchy root CA, including the latter. After the path determination process is complete, the PKIX path validation algorithm is applied.

2.10.4.6 Ants Traversal and Validation

Ants Traversal and Validation (ATV) is proposed as an efficient approach avoiding complexity and trial and error when constructing a certification path. ATV has been published under the title “**ATV: An Efficient Method for Constructing a Certification Path**” in the 18th IFIP World Computer Congress conference [41], and its method of operation is described next. The ATV solution for constructing a path tries to simulate the method used by ants for finding food : a scout is sent to find food, and the scout returns to the colony when it finds food and transmits the information to foragers [28]. In this proposal, the ant model will be altered in order to extend the role of the scout so that they can communicate with foragers. The extended method to be applied as a basis for ATV solution is as follows:

1. The Scout starts the process of constructing the certification path by inspecting the subject's certificate and extracting its information from the repository via LDAP [35].
2. The information is validated to check the status of the subject's certificate:

If the certificate is invalid for any reason (such as having expired), the ATV will end here and a message will be sent to the relying party saying “no reliance can be placed on the target”.

3. The DN attribute is extracted to determine the certificate's issuing CA.
4. The Scout moves to the CA's certificate.
5. Foragers move to the scout's previous position.
6. Foragers look to find any links that connect to their position:
 - a. If there are links, the foragers will also occupy other positions.
 - b. If there are no links, they will stay in their positions.

7. The scout starts to communicate with foragers to detect a suitable path:

A suitable path will be defined using attributes, such as policy constraint, that are defined before the process of construction takes place.

8. If the current position of the scout is a suitable one (i.e. there is an intersection in attributes between the scout and one of the foragers), the following actions are executed:

- a. The scout's certificate will be checked to see if it is self-signed or not.
- b. If self-signed, then a message will be sent to the relying party saying that "the subject certificate is valid".
- c. The certificate will be added to the path.
- d. The ATV will stop.

9. If the scout position is not suitable, then the scout will move to a suitable position which is held by one of the foragers.

10. The path will be modified to include the new certificate and the process begins again at step 3.

2.10.5 Constructing Certification Paths with ATV

In this section we will show how the ATV method is used to construct the certificate path. The following certificate extensions help in building the certification path [1]:

- Certificate policies
- Basic constraints
- Name constraints
- Policy constraints

These extensions have been defined in version 3 of PKI [15, 25], see to table 2-2 for details. We explain how the ATV constructs the certificate path by using name

constraints and certificate policy extensions. We illustrate this by using two examples which explain how ATV constructs the certification path using these constraints.

2.10.5.1 Name Constraints

The name constraints extension (NC) assists in filtering out certificates during the process of constructing the certificate path because each certificate points to its subsequent and preceding certificates. Figure 2-5 shows how the ATV is applied with the name constraints extension, and let us assume that Alice asks to validate certificate 6. As stated previously, ATV has the ability to construct the certification path either forwards or in reverse; the reverse direction is best when constructing certification paths with regard to processing name constraints [26]. To demonstrate the effectiveness of ATV, the following example shows how the algorithm can be applied to the construction of the certification path in a forward direction using the name constraints extension. To simplify this example we have used DNS names and NC to refer to the name constraints extension, as used in [26].

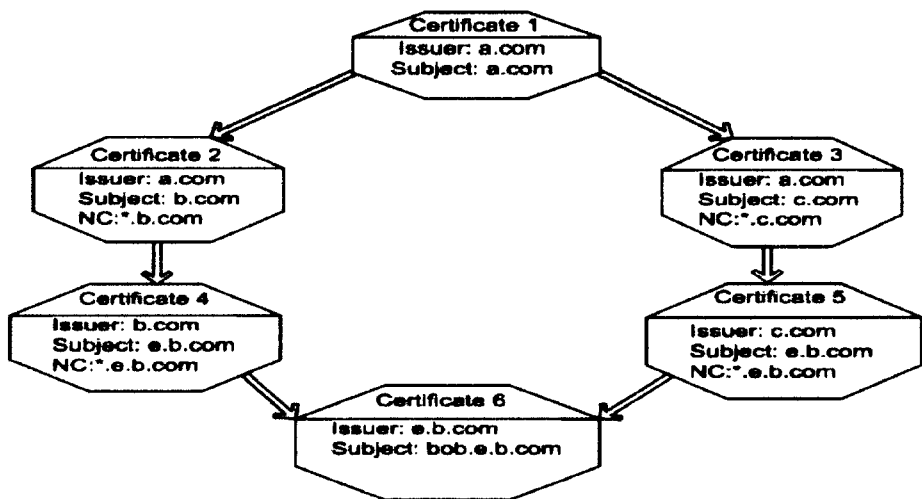


Figure 2-5 Name Constraints Scenario

The scout starts by validating the subject certificate (certificate 6), and after it has retrieved certificate 6's information, the scout moves to certificate 5 and the foragers will land on certificates 6 and 4. When the scout checks the name constraints extension (NC) for certificate 5, it discovers that it is able to reach certificate 6. On the other hand, the forager at certificate 4 also finds that the NC leads to certificate 6. Therefore, the scout and forager at certificate 4 move up one level; the scout then

finds that the NC for certificate 3 does not allow certificate 6 to be reached. Because certificate 2's NC does allow the target certificate to be reached, the scout places itself at certificate 2, and the forager at this certificate will leave certificate 5 because there is no candidate path in the right leg. Finally, the scout moves to certificate 1 which is self-signed and the process of constructing the certification path terminates. The trusted path consists of these certificates: certificate 6 > certificate 4 > certificate 2 > certificate 1.

2.10.5.2 Policy Processing

The certificate policy extension is also used to filter out certificates that do not meet path criteria while in the process of constructing the certificate path. The certificate policy in the subject certificate extension defined by the certificate issuer explains what policies have been followed when issuing the certificate and for what purposes the certificate is suitable. For a CA certificate, the certificate policy extension is used by the issuer to place limitations on the policies that are acceptable in a certification path [26]. How much care the issuer used to authenticate the subject before he issued his certificate is an example of a certificate policy, and (in this example) the level in the certificate policies can be HIGH, MEDIUM or LOW [26].

Figure 2-6 illustrates the use of ATV for constructing a certificate path using certificate policy constraints.

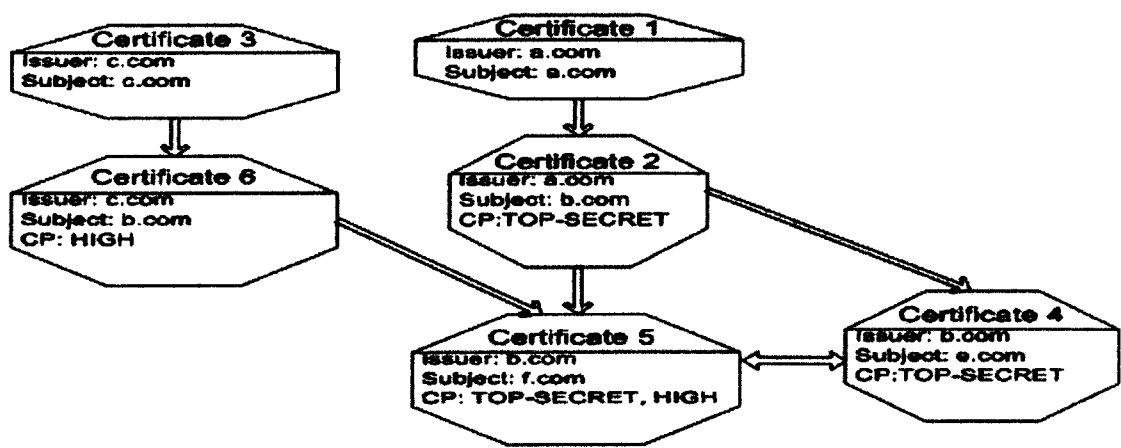


Figure 2-6 Policy Processing Scenario

Let us assume that Alice (the relying party) asks to validate a subject's certificate: certificate 5. The relying party could specify a set of initial policies that she finds acceptable, after a valid path has been built. All the certificates on the valid path must contain these policies. The relying party defines these policies in the policy constraint attribute [26]. In this example the policy constraint attribute is set to HIGH. The scout starts the process of extracting and validating the data of certificate 5. After the scout determines that certificate 5's data is valid, the DN attribute is extracted and the scout moves to certificate 2. Let us assume that certificate 5 has different public keys but the same DN. The foragers now move to certificate 5, and they discover that certificate 5 has three links; because the link toward certificate 2 is being held by a scout, the foragers will move to certificates 4 and 6. The scout starts to communicate with the foragers to determine from the certificate if its CP intersects with the policy constraint attribute. The scout finds that certificate 2 is not the appropriate certificate because TOP-SECRET has no intersection with the policy constraint attribute. Therefore, the scout moves to certificate 6, and finds that the certificate's CP contains HIGH. Because certificate 6 is not self-signed, the scout then moves to certificate 3 and the partial valid path C5>C6 is considered. Certificate 3 is a self-signed certificate, so the validated path is C5>C6>C3 and certificate 5 is considered authenticated; therefore ATV stops.

2.11 Conclusion

The primary focus of this chapter has been Public Key Infrastructure and its associated standards. PKI-enabled security services built on the core PKI services become more useful as they allow secure communications and networking with a broader, global community. The core services are based on the idea of a public-private key pair, which provides support for authentication, encryption, integrity, and non-repudiation. These services enable entities to prove that they are who they claim to be, to secure data during transaction, and to be assured that important data has not been altered in any way, and for no action that took place to be denied. The basis of these security services, PKI architectures, have been discussed with their ways of connecting with each other. This chapter described the PKI system components and their fundamental natures. Certificates that confirm the identity of Internet users were examined next, along with their related operations, issue, revocation, and validation.

Finally, this chapter describes various existing certification path construction methods and our proposed new method.

CHAPTER 3

CERTIFICATE POLICY TECHNIQUES FOR MEASURING TRUST

3.1 Introduction

This chapter explains the concepts behind the CP and CPS, and defines the roles, functions and relationships between them. We mentioned in Chapter 2 that PKI establishes trust and security in the Internet. Trust is represented by certificates that are issued by a CA and they bind information that identifies an entity to a public key and the corresponding private key that the entity controls. The private key is crucial for PKI and must be kept secret. Digital signatures are created by using private key of the sender, while the public key of the receiver is used for encryption. To do business online, PKI users need to have confidence in the certificates that authenticate their remote counterparts, so they need to have confidence that the CA has the proper policies in place to protect users' transaction against unknown threats and vulnerabilities associated with PKI.

The degree of confidence that a certificate user can place on the binding embodied in a certificate depends on several factors [42]:

- CA operating policy, procedures, and security controls which a CA follows when authenticating subscribers.
- Stated obligations and responsibilities of a subscriber such as protecting the private key; and a CA's legal obligations such as warranties and limitations on liability, towards other PKI entities.

Achieving confidence in a PKI is all about addressing the above factors. Stating the obligations and liabilities of all parties involved in an electronic transaction will assist in reducing disputes. PKI requires numerous policies and procedures to maintain the desired level of confidence, for this reason PKI is 10 percent technology and 90 percent policies and procedures, and so is not easy to deploy and maintain [43].

Therefore, confidence is what has been articulated in these policies and procedures, more precisely, it is what is articulated in a CP or a CPS [22].

PKI security could be deficient as a result of a malformed CP and CPS. Organizations that do not properly address security, liability, and obligation issues in their CP and CPS will be excluded from participating in cross-certification by other PKIs. As a consequence, these organizations will lose the ability to conduct secure global transactions, and this will result in them losing subscribers' and relying parties' trust [22].

A CP could be used by a certificate user or relying party as a measurement for deciding whether the binding embodied in a subscriber certificate is trustworthy for a particular application [42].

3.2 Certificate Policy

According to X.509, a CP is "*a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements*". A CP is usually a document written in natural language. Certificate policies extension may declare that one or more specific CPs apply to a subscriber's certificate. Certificates that are applicable to different ranges of applications or purposes are issued following different practices and procedures. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range [15].

Besides the important role of the CP for the relying party, a CA could be audited, accredited, or assessed using the CP. The following scenario makes this clearer: when a subject CA requests a certificate from another CA, the issuer CA must first assess the CPs by which it trusts the subject CA. If the issuer CA trusts the subject CA's CPs, it issues a CA certificate to the subject CA and the subject CA's CPs is indicated in the CA certificate. Afterward, the assessed CPs will be used in the process of constructing certificate paths as accepted policies in certificate policies extensions (see Chapter 2) [42].

3.2.1 A Certificate Policy Example

The following example addresses the use of the CP in industry, and it is cited from RFC3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”:

Suppose that the International Air Transport Association (IATA) undertakes to define some certificate policies for use throughout the airline industry, in a PKI operated by IATA in combination with PKIs operated by individual airlines. Two CPs are defined:

- a. The IATA General-Purpose CP.*
- b. The IATA Commercial-Grade CP.*

The IATA General-Purpose CP could be used by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organization.

The IATA Commercial-Grade CP is used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA requires that certified key pairs be generated and stored in approved cryptographic hardware tokens. Certificates and tokens are provided to airline employees with disbursement authority. These authorized individuals are required to present themselves to the corporate security office, show a valid identification badge, and sign a subscriber agreement requiring them to protect the token and use it only for authorized purposes, as a condition of being issued a token and a certificate.

3.2.2 Object Identifiers

Each CP is assigned a globally unique Object Identifier (OID) which indicates which CP any given certificate follows and which is recognized by both the issuing CA and the relying party. Registration of the Object Identifier is based on the procedures specified in the ISO/IEC and ITU standards. The register also publishes a textual specification of the CP which is used by a relying party when examining the CP. In the case that there is more than one OID in a certificate, the CA informs the certificate user that the certificate is issued in compliance with the asserted policies [22].

3.3 X.509 Certificate Fields

The following extension fields in an X.509 certificate are used to support CPs (see Chapter 2 for more information):

- Certificate policies extension,
- Policy mappings extension,
- Policy constraints extension.

3.3.1 Certificate Policies Extension

The CA lists all the applicable CPs for the certificate in this extension. In the above example, the certificate for regular airline employees, the certificate policies fields contain the object identifier for the General-Purpose policy. However, the certificates of the employees with disbursement authority contain two OIDs (the General-Purpose policy and the Commercial-Grade policy). Two OIDs imply that the certificates are appropriate for either the General-Purpose or the Commercial-Grade policy [42].

3.3.2 Policy Mappings Extension

The Policy Mappings extension provides assurance to a relying party that CPs in other domains will provide equivalent warranties and obligations as the ones in its domain. For example, the ACE Corporation wants to facilitate interoperability and secure their business-to-business exchange with ABC Corporation by cross certification. For this

reason they cross-certify each other's public keys. Both companies have financial transaction protection policies called ace-e-commerce and abc-e-commerce, respectively. To ease the interoperability between the two companies' applications, the policy mapping field could be used in the cross-certificate for the ABC Corporation CA issued by the ACE Corporation CA. This mapping provides a statement that ABC's financial transaction protection policy (i.e., abc-e-commerce) is equivalent to that of the ACE Corporation (i.e., ace-e-commerce). Relying party applications in the ACE domain will accept and rely on certificates issued by the ABC CA [42].

3.3.3 Policy Constraints Extension

The policy constraints extension can be used in certificates issued to CAs and it constraints path validation either by requiring that each certificate in a path contains an acceptable policy identifier or by prohibiting policy mapping [42].

3.4 Certification Practice Statement

The term "certification practice statement" (CPS) is defined by the American Bar Association (ABA) Guidelines as: "*A statement of the practices which a certification authority employs in issuing certificates.*" [44]. As stated above, a CPS focuses on the practice that a CA follows when issuing and managing certificates, including publication and archiving, revocation, and renewal or re-keying [42]. The ABA expands this definition in the Digital Signature Guidelines (DSG) with the following comments [45]:

A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple

documents, a combination of public law, private contract, and/or declaration.

There are cases where a CPS is not needed and could be replaced with a subscriber agreement, relying party agreement, or agreement combining both subscriber and relying party terms, depending on the role of the different PKI participants. [42]:

- 1 In the case that a CA becomes a relying party, the CA is already familiar with the nature and trustworthiness of its services.
- 2 In the case that the issued certificates provide a low level of assurance because the applications are secured and the possibility of compromise may cause marginal risks.

Publishing a full CPS which may address sensitive issues related to the PKI system in addition to provisions that are relevant to the participants in the PKI, could assist an attacker, therefore, the solution is to publish a CPS with only those provisions that are relevant to the participants. This form of CPS is called a “CPS Summary” [42].

3.5 The Relationship between CP and CPS

The CP and CPS are developed to cover different provisions but they address the same topics that interest a relying party when identifying the level of trustworthiness of a public key certificate [42]. A CP is expected to be a higher-level statement than a CPS and it specifies the requirements and standards imposed by the PKI with respect to various topics. It is typically concerned with what participants must do rather than how the participants perform their functions and implement controls. Conversely, a CPS is expected to be an extremely detailed and sensitive document that addresses the internal operating procedures of the CA and/or PKI in addition to the detailed procedures for the life-cycle management of certificates [36].

As the nature of a CP is a statement of requirements, it is suitable as a basis for interoperability between the PKIs of different organizations. A CP in this sense serves as a vehicle for defining the minimum guidelines that must be met by interoperating organizations. Therefore, a CP is able to represent multiple CAs, multiple organizations, or multiple domains. On the other hand, a CPS applies only to a single CA organization and cannot support interoperability. With a single CPS, a CA may

support multiple CPs. A single CP could also be supported by multiple CAs with different CPS [42].

RFC 3647 [42] summarizes the differences between CPs and CPSs in the following:

1. *A PKI uses a CP to establish requirements that state what participants within it must do. A single CA or organization can use a CPS to disclose how it meets the requirements of a CP or how it implements its practices and controls.*
2. *A CP facilitates interoperation through cross-certification, unilateral certification, or other means. Therefore, it is intended to cover multiple CAs. By contrast, a CPS is a statement of a single CA or organization. Its purpose is not to facilitate interoperation (since doing so is the function of a CP).*
3. *A CPS is generally more detailed than a CP and specifies how the CA meets the requirements specified in the one or more CPs under which it issues certificates.*

3.6 Certificate Policy Framework

A Certificate Policy Framework is a “Template” for developing certificate policies; it describes what to include in a CP and/or a CPS. The ultimate goal of the certificate policy framework is to assist writers of CPs and/or CPSs to ensure they cover all areas of technical or legal importance. Moreover, it helps in promoting consistent, comparable certificate policies to assist in cross-certification and policy-mapping decisions [46].

The first document published to assist writers of CPs or CPSs appeared in March 1999 and came from the IETF (the Internet standards body). Amendments to that document were proposed with a comprehensive list of topics in the “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. This document is labelled RFC 2527 and was formalised in April 1998. Since that time this framework has been used by many individuals and organizations representing a variety of different communities developing CPs and CPSs [47].

A new framework, RFC 3647, has been published to replace RFC 2527 and contains incremental improvements. Wide acceptance of RFC 2527 in CP and CPS documents has benefited the development of the new framework. All the improvements that are embedded in the new framework are listed in RFC 3647 under the section “Comparison to RFC 2527”.

3.7 Contents of CP or CPS

The Framework lists all topics that must be covered in a CP definition or a CPS. At the highest level, the topics to be considered include:

1. INTRODUCTION
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES
3. IDENTIFICATION AND AUTHENTICATION
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
6. TECHNICAL SECURITY CONTROLS
7. CERTIFICATE, CRL, AND OCSP PROFILES
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.
9. OTHER BUSINESS AND LEGAL MATTERS

These nine primary components can be used to create a simple CP or CPS. Moreover, they can also be used by a CA to write a subscriber agreement, relying party agreement, or agreement containing subscriber and relying party terms.

Components can be further divided into sub-components, and a sub-component may contain multiple elements. In the case that a component, sub-component, or element has no requirements, a CP or CPS may state “no stipulation”. Therefore it is recommended that all components and sub-components are included in a CP or CPS even if their value is “no stipulation” [42]. Table 3-1 shows the nine components and their subcomponents in accordance with RFC 3647:

Main Components	Subcomponents	
INTRODUCTION	1. Overview 2. Document name and identification 3. PKI participants	4. Certificate usage 5. Policy administration 6. Definitions and acronyms
PUBLICATION AND REPOSITORY RESPONSIBILITIES	1. Repositories 2. Publication of certification information	3. Time or frequency of publication 4. Access controls on repositories
IDENTIFICATION AND AUTHENTICATION	1. Naming 2. Initial identity validation 3. Identification and authentication for re-key requests	
CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	1. Certificate Application 2. Certificate application processing 3. Certificate issuance 4. Certificate acceptance 5. Key pair and certificate usage 6. Certificate renewal	7. Certificate re-key 8. Certificate modification 9. Certificate revocation and suspension 10. Certificate status services 11. End of subscription 12. Key escrow and recovery
FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	1. Physical controls 2. Procedural controls 3. Personnel controls 4. Audit logging procedures	5. Records archival 6. Key changeover 7. Compromise and disaster recovery 8. CA or RA termination
TECHNICAL SECURITY CONTROLS	1. Key pair generation and installation 2. Private Key Protection and Cryptographic Module Engineering Controls 3. Other aspects of key pair management 4. Activation data	5. Computer security controls 6. Life cycle technical controls 7. Network security controls 8. Time-stamping
CERTIFICATE, CRL, AND OCSP PROFILES	1. Certificate profile 2. CRL profile 3. OCSP profile	
COMPLIANCE AUDIT AND OTHER ASSESSMENTS	1. Frequency or circumstances of assessment 2. Identity/qualifications of assessor 3. Assessor's relationship to assessed entity	4. Topics covered by assessment 5. Actions taken as a result of deficiency 6. Communication of results
OTHER BUSINESS AND LEGAL MATTERS	1. Fees 2. Financial responsibility 3. Confidentiality of business information 4. Privacy of personal information 5. Intellectual property rights 6. Representations and warranties 7. Disclaimers of warranties 8. Limitations of liability 9. Indemnities	10. Term and termination 11. Individual notices and communications with participants 12. Amendments 13. Dispute resolution provisions 14. Governing law 15. Compliance with applicable law 16. Miscellaneous provisions 17. Other provisions

Table 3-1 Nine Components with Their Subcomponents

3.8 Major considerations

[22] emphasized that all the required elements of the sub-components listed above are not of equal importance, and it listed topics that to which special attention should be paid during the writing of a CP or CPS. These topics are [22]:

- *Obligations of the various parties, including the CA, RA, subscribers, and the relying party.*
- *Limitations on liability.*
- *Subscriber authentication requirements during initial registration.*
- *Revocation notification procedures (to the relying parties)*
- *Secure audit and secure archive requirements.*
- *Physical, procedural, and personnel security controls at the CA and at the RA.*
- *Technical security controls at the CA, RA, subscribers, especially in the areas of cryptographic module, computer security and network security, and cryptographic token and private protection.*

3.9 Conclusion

In this chapter we discussed the important role of the CP as a factor tending to increase a relying party's confidence. Confidence is increased in an open network such as the Internet when it is known that a CA has employed proper CPs to authenticate its remote counterparts. The CP specifies the requirements such as the obligations and responsibilities of a subscriber (for example, protecting the private key); and the CA's legal obligations (warranties and limitations on liability, etc.), towards other PKI entities. We also discussed how a CP is suitable for supporting interoperability between PKI organizations. The deficiencies of a malformed CP were also described.

The CP applying to a given certificate is distinguished by a globally unique object identifier and we discussed the possibility of certificates having more than one CP. We also showed in this chapter how a CP could be used as the basis for an audit, accreditation, or assessment of a CA. The Certificate extension was introduced in

Chapter 2 but this chapter discusses them again with emphasis on the ones relating to CPs with a concrete explanation of their role. Following this, we introduced the CPS and its implementation, clarifying the relationship between the CP and the CPS. We discuss briefly the framework used to develop CPs and identified the contents of a CP or CPS. Finally, this chapter listed a number of considerations to be taken into account during writing a CP or CPS.

CHAPTER 4

DEVELOPMENT OF THE FORMALISATION METHOD

4.1 Our Approach

CPs are written in natural language, and provide richly detailed and descriptive data scattered throughout the CP document. CPs of this kind are not helpful or efficient for the extraction of data. We aim to formalise and structure the content of the CP to be represented in a systematic way which will ease any process applied to it. We use XML to describe the structure of the CP, as this allows the semantics of the policy to be described: having a description of the CP will facilitate better comprehension of the differences between the subject policy and a specified policy when using a comparison process.

Our work in this chapter is mainly about formalising the CP, and to ensure that this process produces the same formalisation for equivalent CPs. We define a number of conventions to be followed as guidelines during the process. These conventions are:

1. We will use the framework defined in RFC 2527. This outlines the contents of a set of provisions of the CP in the terms of eight primary components.

These components are:

- i. Introduction;
- ii. General Provisions;
- iii. Identification and Authentication;
- iv. Operational Requirements;
- v. Physical, Procedural, and Personnel Security Controls;
- vi. Technical Security Controls;
- vii. Certificate and CRL Profile; and
- viii. Specification Administration.

(a more comprehensive list is available in table 3-1)

2. Where a phrase appears as a section heading, the XML tag consists of those same words, without spaces, and with the first letter of each word (except the first) being capitalised. Thus, for example, the phrase “Community and Applicability” becomes “communityAndApplicability”.
3. We use a fixed value for any expression clause. The value is in string format, with spaces between words e.g. "the sections of EuroPKI-CP".

The formalisation technique that will be applied to encode a CP has developed through three iterations to reach its current, final version. Each stage has been tested and analysed in order to evaluate its applicability to our approach. The following sections contain a more detailed explanation of how each stage was tested and analysed and also illustrate the reasons for producing new versions of the formalisation technique.

4.2 First Version of the Formalisation

At this stage, the process of formalisation has just started and there are several unanswered questions. The most important one was how we were going to perform the formalisation process, and what were the main characteristics of this version of the formalisation? We defined three main guidelines to be followed when performing this stage. These were:

1. The formalisation will be done on the “EuroPKI” Certificate Policy.
2. During the process of formalisation, we will follow the defined conventions.
3. The formalisation will be on the basis of an exact mapping of the CP into XML.

In the next paragraphs we address these concepts in more details:

EuroPKI Certificate Policy

The EuroPKI Certificate Policy has been selected as a model for applying the formalisation technique for the following reasons:

1. [48] states that the EuroPKI is a non-profit organization, and we think this will be a positive point in favour of the CP. This will lead EuroPKI towards developing a high quality of service rather than developing a service for commerce.
2. The EuroPKI policy has been accepted as a Europe-wide standard CP. The widespread of acceptance of EuroPKI encourages us to select it as a reference CP.

Formalisation Conventions

Achieving consistency for the formalisation process requires us to follow the three conventions that have been identified and listed in section 4.1.

Exact Interpretation

The formalisation at this stage was done on the basis of exact interpretation, and this process was carried out by taking each section separately and encoding it in XML.

4.2.1 Applying the formalisation process

We used Stylus Studio 6 (Home Edition) to create the XML presentation, and also to create the XML schema presentation which defines the structure of an XML document through the use of predefined elements; these elements assist in defining the range of valid values for attributes, and the number of times that an attribute can occur. A parser was used to validate the XML documents by comparing them to the XML schema, and if the XML document conforms to the rules of its schema, it is a “valid” XML document [49]. In addition, an XML schema (XSD files) is considered as a database schema which can define the tables, columns and data types for a database; therefore, XSD files provide a model for an XML data document which defines the arrangement of tags and text within all documents referencing the schema [50]. Our target in using the schema was to build a template or framework to be used when comparing it with other policies. The comparison will be done after formalising the target policy in XML, and then applying the comparison process, figure 4-1.

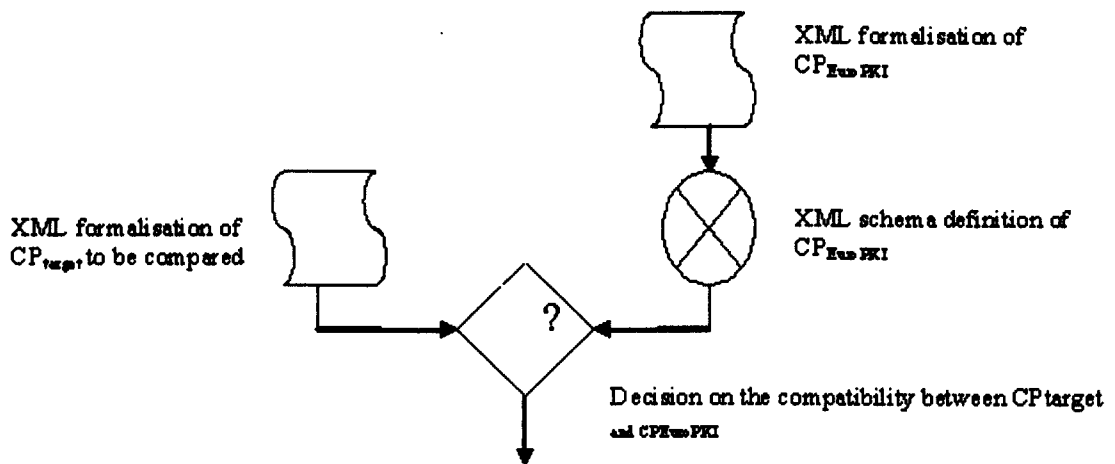


Figure 4-1 Using XML Schema To Perform Comparison

The outcomes of this process were as follows:

- Formalising the whole of the EuroPKI CP.
- Forty documents coded in XML representing the EuroPKI.
- Thirty seven documents in XML schema format (XSD).

The difference in the number of files arose because there are three sections of the EuroPKI CP covering two actions that could be accomplished depending on the circumstances of the decision that had been taken. These two different XML files for the same section are represented by one XSD file that handles both actions (these files are included in the attached CD).

We represented the words that show the requirement levels in our formalisation and we interpreted them as described in RFC 2119 [51] (see Appendix A). These words are:

“MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”,
 “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”,
 “OPTIONAL”.

The following XML representation shows how we use these words represent the requirement levels, emphasising the importance of the action which should be accomplished (**in bold text**).

```
<interpretation of="EuroPKI-CP" accordingToCountryLaw="where conforming CA established">
  <bold>InCPS="MUST"</bold>
</interpretation>
```

An example of the formalisation process, an XML and an XSD file, is given in the next few paragraphs. The following is the XML representation for the EuroPKI CP section entitled “Confidentiality”, and it is followed by the XSD definition:

```
<?xml version="1.0"?>
<confidentiality xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="file:///d:/XML-CP/confidentiality.xsd">
  <CAcollects personalInformation="subscriber">
    <processed withPrivacyProtection="MUST"/>
    <according To="laws" whereCAis="established"/>
  </CAcollects>
  <SubscribersInformation presntInCertificate="false" presntInCRL="false" issuedBy="conforming CA">
    <considered confidential="true"/>
    <resleased to="third parties"
      withExplicitSubscriberAuthorization="SHALL"/>
  </SubscribersInformation>
  <information includedInCertificate="true" includedInCRL="true" issuedBy="conforming CA">
    <considered confidential="false"/>
  </information>
  <when certificate="revoked-suspended">
    <reasonCode included="MAY" inActionEntryOf="CRL">
      <considered confidential="false"/>
    </reasonCode>
    <disclosedOtherDetails>false</disclosedOtherDetails>
  </when>
  <conformingCA disclose="certificate-related OR subscriber personal Information" toThirdParty="false">
    <except requiredBy="law enforcement officials" exhibit="regular warrant"/>
  </conformingCA>
  <releasePartCivil>no stipulation</releasePartCivil>
  <conformingCA-1 disclose="certificate certificate-related information" toThirdParty="false">
    <except requiredBy="owner" with="signed request"/>
  </conformingCA-1>
  <otherCircumstances>no stipulation</otherCircumstances>
  <intellectualPropertyRights>
    <conformingCA calimAnyIPR="MUST NOT" onIssued="certificates"/>
    <anybody allowed="to copy" from="EuroPKI-CPS or EuroPKI-CP" withProviding="a reference to the
      source"/>
  </intellectualPropertyRights>
</confidentiality>
```

This is the XSD definition for the above XML formalisation:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="confidentiality">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="CAcollects">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element name="processed">
                <xsd:complexType>
                  <xsd:attribute name="withPrivacyProtection" type="xsd:string" fixed="MUST"
                                                                use="required"/>
                </xsd:complexType>
              </xsd:element>
              <xsd:element name="according">
                <xsd:complexType>
                  <xsd:attribute name="To" type="xsd:string" fixed="laws" use="required"/>
                  <xsd:attribute name="whereCAis" type="xsd:string" fixed="established"
                                                                use="required"/>
                </xsd:complexType>
              </xsd:element>
            </xsd:sequence>
            <xsd:attribute name="personalInformation" type="xsd:string" fixed="subscriber"
                                                                use="required"/>
          </xsd:complexType>
        </xsd:element>

        <xsd:element name="SubscribersInformation">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element name="considered">
                <xsd:complexType>
                  <xsd:attribute name="confidential" type="xsd:boolean" fixed="true" use="required"/>
                </xsd:complexType>
              </xsd:element>
              <xsd:element name="released">
                <xsd:complexType>
                  <xsd:attribute name="to" type="xsd:string" fixed="third parties" use="required"/>
                  <xsd:attribute name="withExplicitSubscriberAuthorization" type="xsd:string"
                                                                fixed="SHALL" use="required"/>
                </xsd:complexType>
              </xsd:element>
            </xsd:sequence>
            <xsd:attribute name="presntInCertificate" type="xsd:boolean" fixed="false" use="required"/>
            <xsd:attribute name="presntInCRL" type="xsd:boolean" fixed="false" use="required"/>
            <xsd:attribute name="issuedBy" type="xsd:string" fixed="conforming CA" use="required"/>
          </xsd:complexType>
        </xsd:element>

        <xsd:element name="information">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element name="considered">
                <xsd:complexType>
                  <xsd:attribute name="confidential" type="xsd:boolean" fixed="false" use="required"/>
                </xsd:complexType>
              </xsd:element>
            </xsd:sequence>
          </xsd:complexType>
        </xsd:element>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```



```

</xsd:element>
  </xsd:sequence>
  <xsd:attribute name="includedInCertificate" type="xsd:boolean" fixed="true" use="required"/>
  <xsd:attribute name="includedInCRL" type="xsd:boolean" fixed="true" use="required"/>
  <xsd:attribute name="issuedBy" type="xsd:string" fixed="conforming CA" use="required"/>
</xsd:complexType>
</xsd:element>

<xsd:element name="when">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="reasonCode">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="considered">
              <xsd:complexType>
                <xsd:attribute name="confidential" type="xsd:boolean" fixed="false" use="required"/>
              </xsd:complexType>
            </xsd:element>
          </xsd:sequence>
          <xsd:attribute name="included" type="xsd:string" fixed="MAY" use="required"/>
          <xsd:attribute name="inActionEntryOf" type="xsd:string" fixed="CRL" use="required"/>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="disclosedOtherDetails" type="xsd:boolean" fixed="false">
      </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="certificate" type="xsd:string" fixed="revoked-suspended" use="required"/>
  </xsd:complexType>
</xsd:element>

<xsd:element name="conformingCA">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="except">
        <xsd:complexType>
          <xsd:attribute name="requiredBy" type="xsd:string" fixed="law enforcement officials"
            use="required"/>
          <xsd:attribute name="exhibit" type="xsd:string" fixed="regular warrant"/>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="disclose" type="xsd:string" fixed="certificate-related OR subscriber personal
      Information" use="required"/>
    <xsd:attribute name="toThirdParty" type="xsd:boolean" fixed="false" use="required"/>
  </xsd:complexType>
</xsd:element>
<xsd:element name="releasePartCivil" type="xsd:string" fixed="no stipulation">
</xsd:element>

<xsd:element name="conformingCA-1">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="except">
        <xsd:complexType>
          <xsd:attribute name="requiredBy" type="xsd:string" fixed="owner" use="required"/>
          <xsd:attribute name="with" type="xsd:string" fixed="signed request"/>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>

```

```

        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="disclose" type="xsd:string" fixed="certificate certificate-related information"
        use="required"/>
    <xsd:attribute name="toThirdParty" type="xsd:boolean" fixed="false" use="required"/>
</xsd:complexType>
</xsd:element>

<xsd:element name="otherCircumstances" type="xsd:string" fixed="no stipulation">
</xsd:element>

<xsd:element name="intellectualPropertyRights">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="conformingCA">
                <xsd:complexType>
                    <xsd:attribute name="calimAnyIPR" type="xsd:string" fixed="MUST NOT" use="required"/>
                    <xsd:attribute name="onIssued" type="xsd:string" fixed="certificates" use="required"/>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="anybody">
                <xsd:complexType>
                    <xsd:attribute name="allowed" type="xsd:string" fixed="to copy" use="required"/>
                    <xsd:attribute name="from" type="xsd:string" fixed="EuroPKI-CPS or EuroPKI-CP"
                        use="required"/>
                    <xsd:attribute name="withProviding" type="xsd:string" fixed="a reference to the source"
                        use="required"/>
                </xsd:complexType>
            </xsd:element>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:schema>

```

During the formalisation process we had a problem with repeating words (such as entity name, verbs, section name, etc.) in the XML presentation which prevented the validation of the XML documents. We altered our naming system by adding “-*number*” in the case of repeating occurrences; for example, in the above XML formalisation the word “conformingCA” occurs twice, so we named the subsequent one “conformingCA-1”.

To satisfy our goal of defining a framework or template by using the schema, we constructed a single XSD file “EuroPKI-CP.xsd” that contains all the XSD files (included on the attached CD).

4.2.2 Testing the Formalisation

After finishing this first version of the formalisation, the general picture became much clearer. We reviewed the whole formalisation process and especially its outcomes. There are forty XML files representing the EuroPKI CP, and these files are an exact representation of the EuroPKI text in XML. If we recall, our goal beyond establishing the formalisation was to represent the semantics contained in the textual representation of the CP. After reviewing the outcomes, however, we found that we had deviated from this main objective, and we decided that we needed to alter our formalisation process to adapt the representation of the semantics. Therefore, first we needed to define how we could represent the semantics in our presentation.

4.3 Second version of the formalisation

The ultimate aim of this stage is to develop our XML formalisation to be able to represent the semantics articulated in the CP. And as we stated in above, it is necessary first to define what it is that we will use to represent the semantics before a new version of formalisation can be considered. The following section discussed this issue.

4.3.1 Representing Semantics

Words that indicate requirement level (hereafter we call them **obligation words**) are really a type of scale to emphasize the importance of the obligation stated in the CP, and as is stated in [51]:

The force of these words is modified by the requirement level of the document in which they are used.

In the first version of the formalisation, we formalised the whole EuroPKI CP and we found that obligation words had been used to emphasize the level of importance. Also, we realized that, in our case, the semantics are represented by defining what is allowed and what is prohibited for the entity to do in a compliance with the issuer's operating CP. This understanding

matches completely the function of the obligation words that indicate requirement level in the following sense: if the word indicating the requirement level is “**MUST**” this means that the entity is allowed to perform the obligation (indeed, it has to). On the other hand, if the code indicating the requirement level is “**MUST NOT**” in this case the entity is not allowed to perform this action. For this reason, we decided to base our new formalisation on the obligation words, such that this new formalisation would give the obligation words a significant role in showing the importance of each obligation and also representing what is allowed and what is prohibited for an entity.

4.3.2 Obligation Title

Having decided to use the obligation words to represent the semantics, it is necessary to introduce a suitable way of representing them in XML. Accordingly, we have introduced a tag corresponding to each of the obligation words as following:

1. **REQUIREMENT**: **MUST**, **REQUIRED** and **SHALL**.
2. **PROHIBITION**: **MUST NOT** and **SHALL NOT**.
3. **PREFERRED**: **SHOULD** and **RECOMMENDED**.
4. **NOT PREFERRED**: **SHOULD NOT** and **NOT RECOMMEND**.
5. **POSSIBLE**: **MAY** and **OPTIONAL**.

These five words will appear as main sub-sections under each section of the CP, and we will call these words the **obligation title**. All the obligations will be listed in the appropriate obligation title according to their importance as defined in the CP. For example, the obligations section in EuroPKI CP has a sub-section called CA obligations, and the XML representation of the obligations title in this section would be as follows:


```

<obligations>
  <CAObligations>
    <requirement>
      .
    </requirement>
    <prohibition>
      .
    </prohibition>
    <preferred>
      .
    </preferred>
    <notPreferred>
      .
    </notPreferred>
    <possible>
      .
    </possible>
  </CAObligations>
</obligations>

```

As illustrated, the internal sections headed by the obligation title show the obligations upon the CA; therefore if there is a required action that should be taken by the CA, it will be listed under the requirement section. Each obligation title contains a description of what is required under this clause. The presentation of these obligations will be in the following format:

```

<CP section title tag>
  <Entity name tag>
    <Obligation title tag>
      <Description of the obligation>

```

The description section of the obligation will start with a *verb* which describes the action to be taken to perform the obligation, which is then followed by operands and other values. For example, one of the CA obligations states that “CA SHALL operate a certification authority service” and the XML representation for this will be as the following:

```

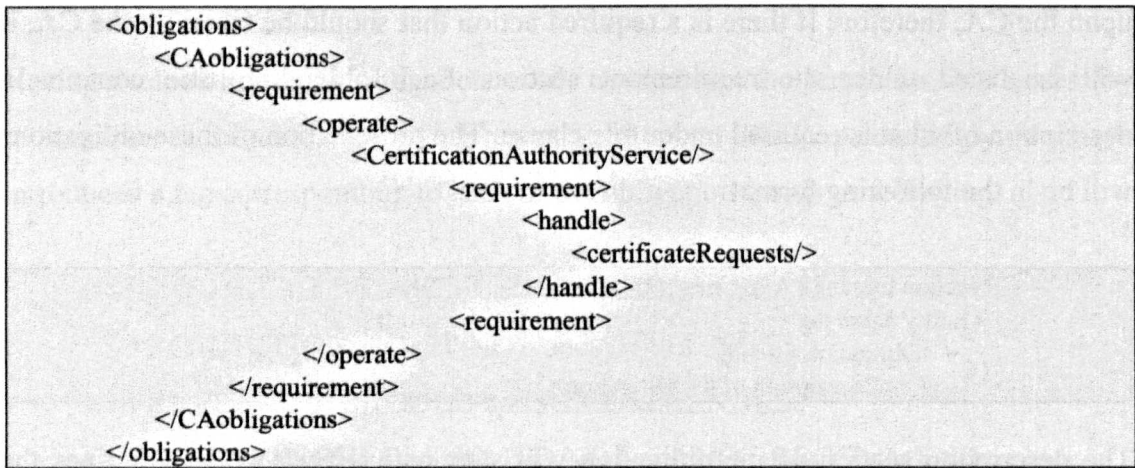
<obligations>
  <CAObligations>
    <requirement>
      <operate>
        <CertificationAuthorityService/>
      </operate>
    </requirement>
  </CAObligations>
</obligations>

```

We observe that the description section of the obligation starts with the verb “operate” under requirement section, and the operand is “CertificationAuthorityService”. In the case where there is another obligation which acts as a constraint on the entity, we can use the obligation tag as a sub-section under the verb. As an example, let us develop the previous example where an obligation was put on the CA to operate a certification authority service. There is a further obligation on this service that states:

Handle certificate request

This represents an additional obligation on the operation of the previously mentioned certification authority service. This obligation will be written with the previous representation, thus:



We can continue using this technique to a greater depth if there are inner obligations.

4.3.3 Formalisation Conventions

As we said in section 4.2, we want to achieve consistency in our formalisation process and for this reason we defined the conventions that we use in our formalisation process. In addition to the previously mentioned conventions, we will also add the following seven new conventions to the current iteration of our formalisation:

1. The formalisation process will be applied to the obligations that have been listed in the CP, and the process will exclude any type of definition.

2. All obligations on an entity; i.e. Certification Authority; will be grouped under the entity's name as a title. For example (in bold text):

```

<CertificationAuthority>
  <requirement>
    <create>
      <certificates/>
    </create>
  </requirement>
</CertificationAuthority>

```

3. If the policy describes obligations for a different entity to the entity that titles the section, all the obligations will be grouped under the different entity's name, such as (different entity in bold text):

```

<operationalAuthority>
  <requirement>
    <IllinoisDepartmentOfCentralManagementServices>
      <serve>
        <asTheOperationalAuthority/>
      </serve>
    </IllinoisDepartmentOfCentralManagementServices>
  </requirement>
</operationalAuthority/>

```

4. Any text in the policy that does not fall in the previous rules will be encoded as comments in the section that it refers to.
5. If there is an inner condition, it will be represented by an inner **obligation title** followed by the entity's name (in bold text):

```

<use>
  <oneOrMore representativesOrAgents="to perform its obligations"
    under="SOIllinois-CP"/>
  <requirement>
    <CA>

```

6. Any obligation in the policy that does not include any of the obligation words, will be treated as a fact which means that the obligations in the text will be listed in the requirement section. Such an example is:

The assigned staff operate the CA functions on a best-effort basis only.

7. If there is a negative word in front of the verb, both of the words will be combined together to form one word (in bold text):

<possible>
 <certificates>
 <notBeUsed>

4.3.4 Tree Representation

The structure of the formalisation developed for the second version leads to a hierarchical tree structure. The tree is be formed by laying down all the entities of the XML representation. The tree root is the name of the CP (EuroPKI-CP in this example – we add CP to distinguish it from a CPS), and the next level will be the CP section names. The third level from top will be the obligation titles, followed by verb tags. The rest of levels will be either the description of the obligation or sub-obligation titles. The following diagram shows the tree presentation for the obligation section of the CAobligations tag - Figure 4-2:

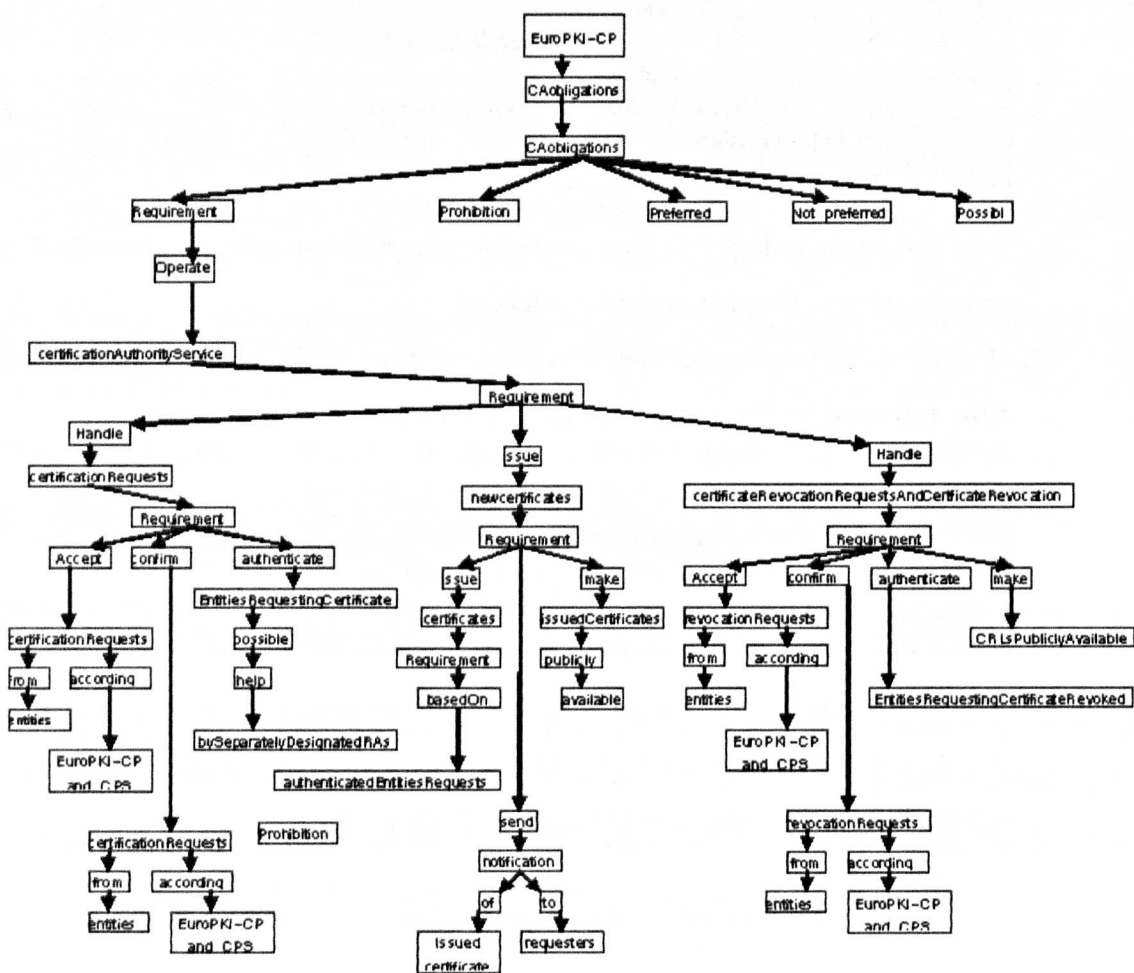


Figure 4-2 Tree Presentation of the CA Obligation Section

We believe that the tree structure will simplify manual comparison when trying to find similarities and differences between a relying party's CP and a subject's CP because it represents clearly all the CP's attributes and their relationships to the obligation title. The following is a tree representation of one obligation of a RA in two different CP's. Figure 4-3:

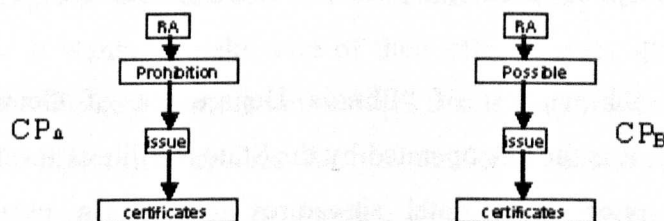


Figure 4-3 Tree Presentation of the Two Different CPs

The above tree presentation show one obligation of the RA entity, and we can observe the difference between the two presentations. CP_A prohibits the RA from issuing certificates; however, CP_B could allow the RA to issue certificates.

The tree structure can also be used to perform automatic compression by encoding the structure using a program. The comparison process could then be done by computer and similarities and differences shown up as a result of this process.

4.3.5 Implementation

We adopted a slightly different scenario when applying the second version of the formalisation. Instead of formalising the whole policy as we did in the first version, we formalised only one section of the CP but for more than one CA. This method helped the comparison of the implementation of the second version on different CPs, and it helped us understand the applicability of this iteration of the formalisation. We chose to apply the formalisation technique to the section called “Community and applicability” of the following five organizations CPs:

1. EuroPKI is a top Level Certification Authority and it offers its services to the members of the Europe Internet community for supporting borderless network security. It offers public-key certification services to public and private organization, as well as to individuals. It wants public-key

certificates to be the main identity identification of individuals, network nodes (e.g. IPsec hosts), and network services (e.g. web servers) [48].

2. DutchGrid as stated in [52] refers to “DutchGrid and NIKHEF medium-security Certification Authority”. This CA is operated by the Certification Authorities group of the Dutch National Institute for Nuclear and High-Energy Physics (NIKHEF) as a courtesy service to the DutchGrid community.
3. CMS is abbreviation of “Illinois Department of Central Management Services”; it is the CA operated by the State of Illinois for digital certificates for encryption and digital signatures for use in providing electronic identification of end-entities as required for conducting State business [53].
4. SwUPKI stands for “the Public Key Infrastructure for Swedish Universities and University Colleges”. It is the CA for the members of SwUPKI. The SwUPKI only includes Swedish universities or university colleges accredited by the Swedish government and related organisations complying with SwUPKI’s CP [54].
5. VeriSign, Inc. is a well-known company offering PKI services. Its services are global and VeriSign Trust Network (VTN) is one of these services. It is a global PKI that accommodates a large, public, and widely distributed community of users with diverse needs for communications and information security [55].

We based our selection of these five organizations on the thought that they will be concerned about the need for a well-defined CP, and therefore important and crucial issues ought to be covered in their CP. To justify our claim let us look closer at them to study their role in the communities they serve.

1. EuroPKI, as we stated above, is a non-profit organization and its primary purpose is to offer public-key certification services to the European Internet community. As we said it will focus on the quality in its offering services to secure the European network.
2. DutchGrid is also a non-profit organization and its service is dedicated to DutchGrid’s members. Therefore, DutchGrid will do its best to offer

sophisticated services that respond to the needs of the DutchGrid's members in providing them with assistance in securing their transactions.

3. CMS represents the State of Illinois government which is the regulator of services for the State of Illinois government. One of these services is offering public-key certification services. As part of the government which is a non-profit organization it is concerned mainly with the quality of its services. It wants to make sure of their effectiveness and especially in the case of public-key certification services that maintain security for all users.
4. SwUPKI offers its services for the academic sector which include the universities and colleges in Sweden. SwUPKI is considered a non-profit organization because its services are bound to specific users, and accordingly it will make sure that its services are adequate, efficient and reliable to meet the needs for securing private individuals transactions.
5. VeriSign, Inc., it is the only commercial organization included because of its good reputation. It is a leading provider of trusted infrastructure services to websites, enterprises, electronic commerce service providers, and individuals. It has its own PKI infrastructure known as the VeriSign Trust Network ("VTN"). An organization with this solid background in PKI services will want to maintain robust services.

This all makes it possible to have well-defined content for the CPs of each organization. The formalisations of the section "Community and applicability" for the organizations' CPs are presented in the paragraphs below.

First EuroPKI's CP:

```
<?xml version="1.0"?>
<EuroPKI-CP>
  <communityAndApplicability>
    <conformingCA>
      <requirement>
        <respect>
          <allLimitation ImposedBy="the sections of EuroPKI-CP"/>
        </respect>
      </requirement>
      <prohibition>
        <issue>
          <certificatesToEntitY doNotBelong="to its community"/>
          <certificatesToApplication haveNotBeen="carefully evaluated"/>
        </issue>
      </prohibition>
    </conformingCA>
  </communityAndApplicability>
</EuroPKI-CP>
```



```

</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
  <choose>
    <for theirCertificates="the community and applicability"/>
    <requirement>
      <specify>
        <in CPS="the community and applicability"/>
      </specify>
    </requirement>
  </choose>
</possible>
</conformingCA>

<CertificationAuthority>
  <requirement>
    <conformingCA>
      <take>
        <careWhen decide="subordinate CA"/>
        <requirement>
          <making>
            <sure candidate="organization or individual" performingAll="controls and checks detailed in
            EuroPKI-CP"/>
          </making>
        </requirement>
      </take>
    </conformingCA>

    <subordinateCAs>
      <sign>
        <agreement with="certifying CA"/>
        <requirement>
          <stating>
            <obligation toAdhereTo="the agreed procedures"/>
          </stating>
        </requirement>
      </sign>
    </subordinateCAs>
  </requirement>
</prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
  <conformingCA>
    <use>
      <As many="RAs as it wishes"/>
    </use>
    <fulfill>
      <theRole of="RA"/>
      <requirement>
        <perform>
          <authentication of="entity"/>
        </perform>
      </requirement>
    </fulfill>
  </conformingCA>

```

```

        </perform>
      </requirement>
    </fulfill>
  </conformingCA>
</possible>
</CertificationAuthority>

<registrationAuthorities>
  <requirement>
    <perform>
      <physical identificationAndAuthenticationOf="entities"/>
    </perform>
    <sign>
      <agreement with="certifying CA"/>
      <requirement>
        <stating>
          <obligation toAdhereTo="the agreed procedures"/>
        </stating>
      </requirement>
    </sign>
  </requirement>
  <prohibition>
    <issue>
      <certificates/>
    </issue>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</registrationAuthorities>

<endEntities>
  <requirement>
    <perform>
      <cryptographicOperations/>
    </perform>
    <conformingCA>
      <detail>
        <inCPS endEntities="that is is willing to certify"/>
      </detail>
    </conformingCA>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</endEntities>

<applicability>
  <requirement>
    <CA>

```



```

        <support>
            <S-MIME/>
            <IPsec/>
            <SSL-TLS/>
        </support>
    </CA>
</requirement>
<prohibition>
    <use>
        <certificates inWay="prohibited by law of countries" where="issuing CA is established"/>
    </use>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</applicability>
</communityAndApplicability>
</EuroPKI-CP>

```

DutchGrid's CP:

```

<?xml version="1.0"?>
<DutchGrid-CP>
    <communityAndApplicability>
        <CertificationAuthorities>
            <requirement>
                <!-- Certification Authorities are only persons. The current list of persons comprising the operational staff of
                the DutchGrid medium-security Certification Authority is published in an on-line accessible repository.
                The location of this list is stated as part of the CPS in section 1.4.-->
            <issue>
                <certificates of="the DutchGrid medium-security Certification Authority"/>
            </issue>
            <assigned>
                <staffMembers responsibleFor="the operational service of the DutchGrid medium-security Certification
                Authority"/>
            </assigned>
            <assignedStaff>
                <operate>
                    <theCAfunctions on="a best-effort basis only"/>
                </operate>
            </assignedStaff>
        </requirement>
        <prohibition>
            <issue>
                <certificate through="automated way"/>
            </issue>
            <NIKHEFcollaboration>
                <held>
                    <liable for="any damages" resultingFrom="the operation or non-operation of the DutchGrid medium-
                    security Certification Authority"/>
                </held>
            </NIKHEFcollaboration>
            <foundationFOM>

```



```

    <held>
      <liable for="any damages" resultingFrom="the operation or non-operation of the DutchGrid medium-
                                                security Certification Authority"/>
    </held>
  </foundationFOM>
  <NIKHEFpartners>
    <held>
      <liable for="any damages" resultingFrom="the operation or non-operation of the DutchGrid medium-
                                                security Certification Authority"/>
    </held>
  </NIKHEFpartners>
  <subordinateCertificationAuthorities>
    <allowed>
      <underDutchGrid-CP/>
    </allowed>
  </subordinateCertificationAuthorities>
  <!-- Distributed validation will be implemented using a network of trusted registration authorities (RA's)-->
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</CertificationAuthorities>

<registrationAuthorities>
<!-- Individuals or groups of individuals can be recognised by the DutchGrid medium-security Certification
                                                Authority-->
  <act>
    <asTrustedIntermediaries in="the identity verification process" between="subscriber and certification
                                                authority"/>
  </act>
  <!--such trusted intermediaries are formally assigned by the CA and their identities and contact details
    published in an on-line accessible repository, the location of which is stated in section 1.4. -->
  <sign>
    <aDocument declaring="their understanding" of="and adherence to DutchGrid-CP/CPS"/>
  </sign>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</registrationAuthorities>

<endEntities>
  <requirement>
  <!--Certificates can be issues to natural persons and to computer entities. The entities that are eligible for
    certification by the DutchGrid medium-security Certification Authority are:-->
  <include>
    <allThoseEntities relatedTo="organisations, formally based in and/or having offices inside the
                                                Netherlands"/>
  </include>
  <requirement>

```

```

    <involved>
      <inTheResearch/>
      <deployment Of="multi-domain distributed computing infrastructure, intended for
                                crossorganisational sharing of resources"/>
      <!-- The focus of these organisations should also be in research and/or education.-->
    </involved>
  </requirement>
  <allThoseEntities associatedto="the DutchGrid platform"/>
  <allOrganisations located="in the Wetenschappelijk Centrum Watergraafsmeer in Amsterdam that are run
                                entirely on a non-for-profit basis"/>

</include>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</endEntities>

<applicability>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
    <certificates>
      <notBeUsed>
        <forFncialTransactions/>
      </notBeUsed>
      <Used>
        <forAnyApplication thatIs="suitable for X.509 certificates"/>
        <prohibition>
          <used>
            <forFncialTransactions/>
          </used>
        </prohibition>
      </Used>
    </certificates>
  </possible>
</applicability>
</communityAndApplicability>
</DutchGrid-CP>

```

CMS's CP:

```

<?xml version="1.0"?>
<SOfillinois-CP>
  <roleIdentification>
    <CertificationAuthority>

```



```

<!-- Where necessary, this Policy distinguishes the different users and roles accessing the CA functions. Where
this distinction is not required, the term CA shall refer to the total CA entity, including the software and its
operations. -->
<requirement>
  <create>
    <certificates/>
  </create>
  <sign>
    <certificates/>
  </sign>
  <distribute>
    <certificates/>
  </distribute>
  <revoke>
    <certificates/>
  </revoke>
  <bind>
    <theX.500DistinguishedNameOfSubscribersAndRegistrationAuthorities with="their respective signature
    verification key and their public encryption key"/>
  </bind>
  <publish>
    <certificateStatus through="certificate revocation lists (CRLs)"/>
  </publish>
  <design>
    <itsCertificationPractice to="reasonably achieve the requirements of SOfillinois-CP"/>
  </design>
  <implement>
    <itsCertificationPractice to="reasonably achieve the requirements of SOfillinois-CP"/>
  </implement>
  <operate>
    <itsCertificationPractice to="reasonably achieve the requirements of SOfillinois-CP"/>
  </operate>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
  <use>
    <oneOrMore representativesOrAgents="to perform its obligations" under="SOfillinois-CP"/>
    <requirement>
      <CA>
        <remain>
          <responsibleFor complying="with SOfillinois-CP"/>
        </remain>
      </CA>
    </requirement>
  </use>
  <issue>
    <cross-certificates to="other CAs"/>
    <requirement>
      <CA>
        <authorized>
          <expressly by="the Policy Authority"/>
        </authorized>
      </CA>
    </requirement>
  </issue>

```

```

        <!-- Cross-certificates will be issued to other CAs where a crosscertification agreement has been
              developed between the PA and the policy governing body of the other CA. Cross-certification will
              be implemented according to the requirements defined in that agreement -- ->
    </requirement>
</issue>
</possible>
</CertificationAuthority>

<PolicyAuthority>
  <requirement>
    <responsible>
      <forEnsuring thatBoth="the policy and the practices that the CA employs in issuing certificates"
        areConsistentWith="the policies described in SOfillinois-CP"/>
    </responsible>
    <consist>
      <ofIndividuals representing="constitutional offices, state agencies, and local governments"
        whichAreUtilizing="the State of Illinois public key infrastructure"/>
    </consist>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</PolicyAuthority>

<operationalAuthority>
  <requirement>
    <IllinoisDepartmentOfCentralManagementServices>
      <serve>
        <asTheOperationalAuthority/>
      </serve>
    </IllinoisDepartmentOfCentralManagementServices>
    <responsible>
      <for theOperationOf="the CA in accordance with SOfillinois-CP and the practices described in the CPS"/>
    </responsible>
    <make>
      <aCopy of="SOfillinois-CP" available="to all End-Entities within its CA"/>
    </make>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</operationalAuthority>

<registrationAuthorities>
  <requirement>
    <StatePA>
      <appoint>
        <atLeastOneRA/>

```



```

    </appoint>
    <responsible>
      <for theIdentificationAndAuthenticationOf="End-Entities" inAccordanceWith="SOfillinois-CP"/>
    </responsible>
  </StatePA>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</registrationAuthorities>

<LocalRegistrationAuthorities>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
    <eachStateAgency>
      <participat>
        <inTheStatePKI/>
      </participat>
      <andOtherEntities>
        <determined>
          <byThePA/>
        </determined>
        <appoint>
          <oneOrMoreLRAs/>
        </appoint>
      </andOtherEntities>
    </eachStateAgency>
    <responsible>
      <for theIdentificationAndAuthenticationOf="End-Entities within the Agency organization"
        inAccordanceWith="SOfillinois-CP"/>
    </responsible>
  </possible>
</LocalRegistrationAuthorities>

<endEntities>
<!-- At the discretion of the PA, any person entity, hardware device or specific application may be a Subscriber or
  Relying Party (collectively referred to as an End Entity ) in the State PKI -->
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>

```

```

<include>
  <stateEmployees/>
  <individuals>
    <requirement>
      <conduct>
        <electronicBusiness with="the State"/>
      </conduct>
    </requirement>
  </individuals>
  <hardwareDevices/>
  <specificApplications/>
</include>
<use>
  <certificates issued="by the CA to encrypt information" for="other End-Entities within the State PKI"/>
</use>
<verify>
  <theDigitalSignatures of="other End-Entities within the State PKI"/>
</verify>
</possible>
</endEntities>

<repositories>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</repositories>

<sponsors>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</sponsors>

<subscribers>
<!-- The Subscriber agreement may be viewed at http://www.illinois.gov/pki/pki\_subscriber.cfm -->
  <requirement>
    <SOIllinois-CP>
      <bind>
        <onEachSubscriber that="applies for and/or obtains Certificates" byVirtue="of the Subscriber
                                                                    Agreement"/>
      </bind>
      <govern>
        <eachApplicantPerformance with="respect to their application for, use of, and reliance on,
                                                                    Certificates" issuedBy="the CA"/>
      </govern>
    </SOIllinois-CP>
  </requirement>

```



```

    </bind>
  </SOIllinois-CP>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</subscribers>

```

```

<RelyingParties>

```

```

<!-- Any entity that has received a certificate and a digital signature verifiable with reference to a public key listed
in the certificate -->

```

```

  <rely>
    <onCertificateAandDigitalSignature/>
  </rely>
  <agree>
    <toBeBound by="the terms of SOIllinois-CP and the CPS"/>
  </agree>
  <agree>
    <toBeBound by="the provisions of SOIllinois-CP"/>
  </agree>
  <requirement>
    <relyingParty>
      <accept>
        <certificate issued="pursuant to the provisions of SOIllinois-CP"/>
      </accept>
    </relyingParty>
  </requirement>
  <prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>

```

```

<!-- The following factors, among others are significant in evaluating the reasonableness of a recipient's
reliance upon a certificate, and upon digital signatures verifiable with reference to the public key listed in
the certificate:

```

- (1) Facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference;
- (2) The value or importance of the digitally signed message, if known;
- (3) The course of dealing between the relying person and the subscriber, and the available indicia of reliability or unreliability apart from the digital signature;
- (4) The usage of trade, particularly trade conducted by trustworthy systems or other computer based means -->

```

</RelyingParties>
</roleIdentification>
</SOIllinois-CP>

```

SwUPKI's CP:

```

<?xml version="1.0"?>
<SwUPKI-CP>
  <communityAndApplicability>
    <PolicyManagementAuthority>
      <requirement>
      </requirement>
      <prohibition>
      </prohibition>
      <preferred>
      </preferred>
      <notPreferred>
      </notPreferred>
      <possible>
      </possible>
    </PolicyManagementAuthority>

    <CertificationAuthority>
      <requirement>
        <creat>
          <certificates/>
        </creat>
        <sign>
          <certificates/>
        </sign>
        <bind>
          <Subscribers to="the public signature verification keys attributable to them"/>
          <PKIpersonnel to="the public signature verification keys attributable to them"/>
          <otherCAs to="the public signature verification keys attributable to them"/>
        </bind>
        <provide>
          <CertificateRepositoryAndCertificateStatusService/>
        </provide>
        <publish>
          <CPS>
            <requirement>
              <include>
                <reference to="SwUPKI-CP"/>
              </include>
            </requirement>
          </CPS>
        </publish>
        <assign>
          <duties to="its RAs"/>
          <!-- ,and for the compliance with this CP by the CA itself, its RAs and any subordinate CAs -->
        </assign>
      </requirement>
      <prohibition>
      </prohibition>
      <preferred>
      </preferred>
      <notPreferred>
      </notPreferred>
      <possible>
        <notAssign>
          <duty ofIssuingCertificatesTo="RA"/>
        </notAssign>
        <use>
          <!-- While an Organisation in the PKI may use a contractor to provide (some of its) CA services, it remains

```


responsible and accountable for the operation of its CA. -->

```
<contractor to="provide CA services"/>
  <requirement>
    <responsible>
      <for theOperationOf="its CA"/>
    </responsible>
    <accountable>
      <for theOperationOf="its CA"/>
    </accountable>
  </requirement>
</use>
<do>
  <!-- Cross-certification under this CP, with CAs external to SwUPKI, may only be done by the Policy CA
  after decision by the PMA, and shall comply with this CP and any additional requirements decided by the
  PMA.-->
  <cross-certification through="the Policy CA" with="CAs external to SwUPKI"/>
    <requirement>
      <after decision="by the PMA"/>
      <comply with="SwUPKI-CP"/>
      <anyAdditionalRequirements decidedBy="the PMA"/>
    </requirement>
  </do>
</possible>
</CertificationAuthority>

<registrationAuthorities>
  <requirement>
    <responsible>
      <forAllDuties assignedToItBy="CA"/>
      <requirement>
        <operate>
          <inCompliance with="SwUPKI-CP"/>
        </operate>
      </requirement>
    </responsible>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
    <notIssue>
      <certificates/>
    </notIssue>
  <perform>
    <duties onBehalfOf=" more than one CA"/>
    <requirement>
      <satisfies>
        <all theRequirementsOf="SwUPKI-CP"/>
      </satisfies>
    </requirement>
  </perform>
  </possible>
</registrationAuthorities>

<endEntities>
```

```

<requirement>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</endEntities>

<repositories>
  <requirement>
    <CA>
      <ensure>
        <there is="Certificate repository and a Certificate Status Service (CSS)"/>
        <requirement>
          <CSS>
            <associated>
              <withIt/>
            </associated>
            <consistsOf>
              <CRLrepository/>
            </consistsOf>
          </CSS>
          <comply>
            <with currentStandardsAsStatedIn="the CPS"/>
          </comply>
        </requirement>
        <possible>
          <CSS>
            <consistsOf>
              <OnlineCertificateStatusService/>
            </consistsOf>
          </CSS>
        </possible>
      </ensure>
    </CA>
  </requirement>
</prohibition>
</prohibition>
</preferred>
</preferred>
</notPreferred>
</notPreferred>
</possible>
</possible>
</repositories>

<sponsors>
  <requirement>
    <eachOrganisation>
      <issuing>
        <certificates/>
      </issuing>
    </eachOrganisation>
    <supplyOrConfirm>

```



```

    <authenticationAndCertificateAttributeDetails to="the CA or RA"/>
  </supplyOrConfirm>
  <inform>
    <theCAorRA>
      <ifTheSponsorRelationship with="the Subscriber terminates Or changes"/>
        <requirement>
          <revok>
            <certificates/>
          </revok>
        </requirement>
      </theCAorRA>
    </inform>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
    <suggest>
      <appropriateDistinguishedNames for="Subjects"/>
    </suggest>
  </possible>
</sponsors>

<subscribers>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
    <CA>
      <issue>
        <certificates toSubscribers="employees, students, guests and others"/>
        <requirement>
          <having>
            <sponsor within="the Organisation of CA"/>
          </having>
        </requirement>
      </issue>
    </CA>
  </possible>
  <!--Eligibility for a certificate is at the sole discretion of the CA. -->
</subscribers>

<subjects>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>

```

```

</notPreferred>
<possible>
  <CA>
    <issue>
      <certificates whereTheSubjectIs="the Subscriber, an organisational role or an ITsystem"/>
      <requirement>
        <responsibilityAndAccountability>
          <attributable>
            <toTheSubscriber/>
          </attributable>
        </responsibilityAndAccountability>
      </requirement>
    </issue>
  </CA>
</possible>
</subjects>

<applicability>
  <requirement>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  </possible>
</applicability>
</communityAndApplicability>
</SwUPKI-CP>

```

Finally, VeriSign's CP:

```

<?xml version="1.0"?>
<VeriSign-CP>
  <PKI-Participants>
    <CertificationAuthorities>
      <requirement>
        <issue>
          <publicKeyCertificates within="the VTN"/>
        </issue>
        <encompass>
          <aSubcategoryOfIssuers called="Primary Certification Authorities (PCA)"/>
        </encompass>
        <PCAs>
          <!-- Each PCA is a VeriSign entity-->
          <requirement>
            <act>
              <asRoots of="four domains"/>
            </act>
            <contain>
              <CertificationAuthorities>
                <requirement>
                  <issue>
                    <certificates to="end-user Subscribers or other As"/>

```



```

        </issue>
      </requirement>
    </CertificationAuthorities>
  </contain>
</requirement>
</PCAs>
<!-- One VTN CA technically outside the three hierarchies under each of the PCAs is the Secure Server
      Certification Authority. This CA does not have a superior CA, such as a root or a PCA. Rather-->
<SecureServerCertificationAuthority>
  <acts>
    <asItsOwnRoot andHas="a self-signed root certificate"/>
  </acts>
  <issue>
    <certificates to="end-user Subscribers"/>
  </issue>
  <!-- Server Hierarchy consists only of the Secure Server CA-->
  <issues>
    <SecureServerIDs/>
    <!-- which are deemed to be Class 3 Organizational Certificates and are functionally equivalent to
          Certificates issued by a Class 3 CA-->
  </issues>
  <approved>
    <byVeriSignAndDesignated As="a Class 3 CA within the VTN"/>
    <requirement>
      <SecureServerCA>
        <employs>
          <lifecyclePractices that="are substantially similar with those of other Class 3 CAs within the
                VTN"/>
          <!-- The Certificates it issues are considered to provide assurances of trustworthiness
                comparable to other Class 3 organizational Certificates -->
        </employs>
      </SecureServerCA>
    </requirement>
  </approved>
</SecureServerCertificationAuthority>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
  <VeriSignEnterpriseCustomers>
    <operate>
      <theirOwnCAs as="a subordinate CA to a VeriSignPCA"/>
    </operate>
    <requirement>
      <!-- Such a customer enters into a contractual relationship with VeriSign -->
      <abide>
        <byAllTheRequirements of="the VTN CP and the VeriSign CPS"/>
      </abide>
    </requirement>
    <subordinateCAs>
      <implement>
        <aMoreRestrictivePractices basedOn="their internal requirements"/>
      </implement>
    </subordinateCAs>
  </VeriSignEnterpriseCustomers>
</possible>

```

```

    </VeriSignEnterpriseCustomers>
  </possible>
</CertificationAuthorities>

<registrationAuthorities>
  <requirement>
    <perform>
      <identification>
        <ofCertificateApplicants for="end-user certificates"/>
      </identification>
      <authentication>
        <ofCertificateApplicants for="end-user certificates"/>
      </authentication>
    </perform>
    <initiatesOrPasses>
      <alongRevocationRequests for="certificates for end-user certificates"/>
    </initiatesOrPasses>
    <approves>
      <applications for="renewal or re-keying certificates" onBehalfOf="a VTN CA"/>
    </approves>

    <ThirdPartyRAs>
      <abide>
        <byAllTheRequirements Of="the VTN CP , the relevant CPS and any Enterprise Service Agreement
                                                                    entered into with VeriSign"/>
      </abide>
    </ThirdPartyRAs>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
    <VeriSignAndAffiliates>
      <act>
        <asRAs for="certificates they issues"/>
      </act>
    </VeriSignAndAffiliates>
    <ThirdPartyRAs>
      <!--who enter into a contractual relationship with VeriSign or an affiliate-->
      <operate>
        <theirOwnRA/>
      </operate>
      <authorize>
        <theIssuance of="certificates by a VTN CA"/>
      </authorize>
    </ThirdPartyRAs>
    <implement>
      <aMoreRestrictivePractices basedOn="their internal requirements"/>
    </implement>
  </possible>
</registrationAuthorities>

<subscribers>
  <requirement>
    <include>

```



```

    <allEndUsers of="certificates issued by a VTN CA"/>
  </include>
  <!--A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be
    individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other
    devices used to secure communications within an Organization-->
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</subscribers>

<relyingParties>
  <requirement>
    <!--A Relying Party is an individual or entity-->
    <acts>
      <inReliance Of="a certificate and/or a digital signature issued under the VTN"/>
    </acts>
  </requirement>
  <prohibition>
  </prohibition>
  <preferred>
  </preferred>
  <notPreferred>
  </notPreferred>
  <possible>
  <be>
    <aSubscriber within="the VTN"/>
  </be>
  </possible>
</relyingParties>

<otherParticipants>
  <requirement>
    <AnAffiliate>
      <operate>
        <CertificationAuthority under="the VTN within a specific territory"/>
      </operate>
    </AnAffiliate>
    <ProcessingCenters>
      <create>
        <aSecureFacilityHousing/>
      </create>
      <use>
        <theCryptographicModules for="the issuance of Certificates"/>
      </use>
      <act>
        <asCAs within="the VTN"/>
      </act>
      <issu>
        <Certificates/>
      </issu>
      <manag>
        <Certificates/>

```

```

</manag>
<revok>
  <Certificates/>
</revok>
<renew>
  <Certificates/>
</renew>
  <!--Affiliates who outsource the backend functionality to VeriSign but retain the RA responsibilities are
    called Service Centers-->
</ProcessingCenters>
</requirement>
<prohibition>
</prohibition>
<preferred>
</preferred>
<notPreferred>
</notPreferred>
<possible>
</possible>
</otherParticipants>
</PKI-Participants>
</VeriSign-CP>

```

4.3.6 Testing the formalisation

Natural language is ambiguous, imprecise and vague [56], a CP is not a structured document and there is no consistency in CPs because some CAs introduce new entities, which are not defined in RFC 2527 nor found in other CPs, to perform specific tasks. For example, SwuPKI's CP introduces the "Policy Management Authority" entity which is not found in the other CPs. All these factors lead to different representations for the CPs that we formalised, making the comparison process inefficient, so we need a new version of formalisation to overcome this.

4.4 Final version of the formalisation

We observed that identical representations could be obtained by defining certain criteria that have same name in all the formalisation of CPs but differ in their values. The process of defining these criteria is explained in the following sections.

4.4.1 Defining criteria for the comparison process

The process for defining the criteria was started by constructing a table with three columns. Each column contained one of the three CA's CPs, EuroPKI, SwUPKI or

DutchGrid. The aim behind this was to perform a manual comparison between the three CPs to find the criteria that they have emphasised, and those that play a significant role in defining the obligations. The first page of the table is showing in the Figure 4-4. Each row of the table contains one numbered section of each participating CP such as “1.3 Community and applicability” and the following numbered section “1.3.1 Policy Management Authority” is in a different row. We had 106 pages of double-sided A4 landscape-size pages after filling up the table’s rows with the content of the three CPs. In the case where a CP has a numbered section that is not found in other CPs then its row cell was filled and the other cells left empty (see Appendix B).

EuroPKI	SwuPKI	DutchGrid
1.3 Community and applicability A conforming CA can choose freely which are the community and applicability of their issued certificates but it MUST clearly specify them in its own CPE. In every case a conforming CA MUST NOT issue certificates to entities that don't belong to its community or for applications that haven't been carefully evaluated (for instance high value B2B transactions). Moreover a conforming CA SHALL respect all the limitations imposed by the following sections of this policy.	1.3 Community and Applicability This policy is designed for use in SwuPKI. Only Swedish universities or university colleges accredited by the Swedish government and related organisations complying with this CP can be members of SwuPKI. "Organisation" is used to denote a member of SwuPKI.	1.3 Community and Applicability
	1.3.1 Policy Management Authority (PMA) One member of SwuPKI has the specific responsibility of being the Policy Management Authority of the PKI. The PMA is responsible for registering, interpreting and maintaining this CP. Appointing a member of SwuPKI to serve as the Policy CA for SwuPKI. Approving the CPs of CAs in SwuPKI, compliance inspections and general supervision of SwuPKI, cross-certification with other PKIs and with CAs of other PKIs.	

Figure 4-4 First Page of the Table Used To Do Manual Comparison Process

4.4.2 Comparison criteria for the formalisation

When the process of manual comparison was finished, we came up with 43 criteria represented in table 4.1:

Number	Section number	Criterion
1	1.3	Does the CA issue certificate to entities outside its community? Does the CA issue certificate for application that have not been carefully evaluated?
2	1.3.1	Could the CA have the role of RA? Does the CA allow for subordinate CA?
3	1.3.2	Is the RA allowed to issue certificates?
4	13.4	Is there any limitation on the use of the certificates?
5	1.3.5	Does the policy allow for sponsors or introducers?
6	2.1.1	Does the CA ensure that subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End Entity hardware and software used in connection with the PKI? Does the CA manage the certificates in accordance with its CP?
7	2.3	Does the CA provide any financial responsibility?

8	2.4.1	Does national law govern any agreements?
9	2.4.3	Does the CP agree to let an arbitrator to resolve a dispute?
10	2.7	Does the CP allow for external audit or compliance inspection?
11	2.7.1	Is there a frequency for entity compliance inspection?
12	2.7.3	Is there a relationship between the auditor and the audited party?
13	2.7.5	Is there an action taken as a result of deficiency?
14	2.8	Does the CA disclose subscribers' information or certificate-related information to any third parties without explicit subscriber's authorization?
15	2.8.3	Does the CRL entry for action include the reason code?
16	2.8.7	Does a compliance auditor have access to the CA's cryptographic keys?
17	3.1.5	Who judges name claim disputes?
18	3.1.7	Is there a method to prove possession of private key?
19	3.1.8	Does authentication of an organization identity include its popularity in the community?
20	3.1.9	Does authentication of individual identities require that individuals present themselves personally to the authenticating party? Does the authentication process of the individual is recorded?
21	3.2	Does the CP allow for recertification of an existing public key? Is the key re-authentication accomplished by the same procedure as for the initial registration?
22	3.3	Does the CP allow for re-certification of a revoked public key?
23	4.1.1	Does the CP support cross-certification?
24	4.3	Does the CP request for subscriber acknowledge acceptance of certificate and its obligations?
25	4.4	How long does a CRL need to be updated since any revocation of a certificate?
26	4.4.9	Does a CRL have a validation period, and does it last for more than 30 days?
27	4.5.1	Do security audit procedures include all events?
28	4.5.2	Are audit logs periodically reviewed?
29	4.5.8	Does the CP request for the vulnerability assessments?
30	4.6	Does the archival procedure record all events?
31	4.8.4	Is there a disaster recovery plan?
32	5.1.2	Is there physical security controls to control access to the CA site?
33	5.2.1	Does the CP define the trusted roles?
34	5.2.3	Does the CP request for identification and authentication for each role?
35	5.3	Does the CP ask for personnel controls?
36	6.1.1	Does the CA generate the end-entities' cryptographic keys?
37	6.1.5	What is the minimum length for the private key? Does the CA's key length longer than the end entity's key length?
38	6.1.9	Does the CP request for flagging the KeyUsage extension as critical?
39	6.3.2	Does the CP define a usage periods for the public and private keys?
40	6.5.1	Are there specific computer security technical requirements for CA machine?
41	6.6.2	Is there any security management controls?
42	6.6.3	Is there any life cycle security rating?
43	6.7	Does the CP define the network security controls?

Table 4-1 the Criteria That Were Produced By the Manual Comparison Process

These criteria need to be evaluated and analysed to:

1. Filter them, so we consider only the criteria that will satisfy the requirements laid down in the following section.
2. Represent crucial information that is required during authentication which will assist the relying party to make his/her decision to accept or reject a subject's certificate.

4.4.3 Requirements for certification service providers

The Department of Trade and Industry (DTI) has outlined the requirements on certification service providers for issuing qualified certificates in its directive [57] in Annex II. As stated in the Annex, the certification service providers must meet these requirements in order to issue qualified certificates. The requirements cover the following:

Requirement 1: *Demonstrate the reliability necessary for providing certification services.*

Requirement 2: *Ensure the operation of a prompt and secure directory and a secure and immediate revocation service.*

Requirement 3: *Ensure that the date and time when a certificate is issued or revoked can be determined precisely.*

Requirement 4: *Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued.*

Requirement 5: *Employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards.*

Requirement 6: *Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them.*

Requirement 7: *Take measures against forgery of certificates, and, in cases where the certification service-provider generates signature creation data, guarantee confidentiality during the process of generating such data.*

Requirement 8: *Maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance.*

Requirement 9: *Record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically.*

Requirement 10: *Not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services.*

Requirement 11: *Before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily (in the directive written as redily) understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate.*

Requirement 12: *Use trustworthy systems to store certificates in a verifiable form so that:*

- *only authorised persons can make entries and changes,*
- *information can be checked for authenticity,*
- *certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and*
- *any technical changes compromising these security requirements are apparent to the operator.*

We use the DTI requirements to evaluate the criteria, and, moreover, to eliminate unnecessary criteria. Table 4-2 will be used to link the criteria to their corresponding requirements (in correspondence to their numbers, listing only the number that indicates the requirement or criterion):

Requirements	Corresponding criteria
1	
2	25, 26, 31
3	39
4	19, 20
5	35
6	37, 41, 42
7	3, 27, 28, 29, 33, 40, 43,
8	7
9	30
10	14, 36
11	6, 24
12	

Table 4-2 Showing the Relation between Requirements and Criteria

On examining the above table, we found that most requirements are associated with related criteria; and some of them with more than one. On the other hand, there are some requirements not associated with any criteria, as happened with requirements 1 and 12. However, there is one thing we need to note : these 12 requirements were laid down to guide CAs when issuing qualified certificates which means that the CA’s services will be considered as trusted services if it followed these requirements. In this sense, these requirements could be used to evaluate an established CA. The main point here is that the subject which will be evaluated is known to the evaluator, but in our case we are evaluating the subject through the policy that manages the subject’s certificate where the subjects are unknown to us. This leads to two requirements without related criteria and there are also necessary criteria that do not have requirements. We are going to consider requirements 1 and 12 in our criteria. Thawte is a well known company providing certification services and states in [9]

A digital signature is only as reliable as the CA is trustworthy in performing its functions

As Thawte declares this fact about known CAs, this requires us to define three requirements to cover the following issues:

1. The role of national law
2. Dispute resolution procedures
3. Audit service

To tackle these issues, we have defined the following requirements (continuing the consecutive numbering already assigned to the above requirements):

Requirement 13: Consider national law as the superior law for any agreement.

Requirement 14: Allow for arbitration as an alternative dispute resolution mechanism.

Requirement 15: Perform frequent audits of a CA's performance for compliance with the requirements of its CP, carried out by an external auditor, and take action in the case of failure to comply with the CP.

Table 4-3 shows the new relationships. Criteria represented in Table 4-2, are listed using their numbers in the “corresponding criteria” column, but for the criteria that were not represented in table 4-2 we will refer to their section number in the CP:

Requirements	Corresponding criteria
1	1.3.1
12	
13	8
14	9
15	10, 11, 13

Table 4- 3 Showing the New Relation between Requirements and Criteria

Table 4-3 shows that requirement 12 is still without a related criteria. Looking closely at this requirement, we found that its obligations were covered by other requirements. Requirement 12’s obligations talk about:

- Authenticating all access to stored data: covered by requirement 7.

- Authorization in disclosing any confidential information: covered by requirement 10.
- Auditing suspicious activities: covered by requirement 6.

Finally, we have defined the criteria that we will use in our XML formalisation in order to perform the comparison with the subject's CP to define the level of trust that a relying party can place on a subject's CP. The comparison will be accomplished by comparing the pre-defined values for the criteria with the value in the subject's CP. We include 27 criteria in our XML formalisation, and these cover the following issues when we perform the comparison process:

- Capability of a new certification service provider (subordinate CA).
- Quality of the revocation process and continuity after disaster.
- Validity Periods for Public and Private Keys.
- Authenticity procedures.
- Quality of personnel.
- Main security procedures.
- Operational security procedures.
- Financial responsibility.
- Archiving process and its keeping period.
- Privacy protection.
- Obligations and rights of subscriber.
- Subscriber's rights, obligations and liabilities.
- Acceptance of government law.
- Dispute reference.
- Auditing procedures.

The above issues will help us to come to a final decision on a subject's identity and therefore will be able to answer the question about the level of trustworthiness that can be concluded from its CP. In the next chapter we will place the criteria in the formalisation and examine them further.

4.5 Conclusion

This chapter is the core chapter where we carried out the process of formalising the CP. The process ran in 3 stages, each is explained, tested and the reason for initiating the next stage is given. The first phase of the formalisation was an exact interpretation of the textual form of the EuroPKI CP. With five different CPs, the formalisations in the second phase were non-identical which definitely did not assist the comparison process. In the final phase, a manual comparison was carried out between three different CPs, and this resulted in defining 27 criteria. Before we started formalisation process, we defined a number of conventions on which to base our formalisation so as to produce identical formalisations. In the final formalisation stage, a filtering process was applied to the 43 criteria to remove unrelated criteria, and to represent crucial information required for the comparison process. We added essential requirements to cover the case of authentication of unknown certification service providers.

CHAPTER 5

REPRESENTING THE CRITERIA IN THE XML FORMALISATION

5.1 Introduction

In this chapter we first explain the semantics behind each of the defined criteria, and then specify their XML representations. In addition, we define a numerical evaluation system that will be used as a rating system for each subject criterion. Finally as an end to the comparison process, we define the comparison results which fall into one of the following cases: no overlap, absolute overlap, partial.

5.2 The Semantics behind the Criteria

The overall objective of the criteria is to provide an extra level of assurance about the subject's certificate as well as the assurance of the CA that vouches for the identity of the subject to whom it issues a certificate. On the other hand, to know the detailed objectives of these criteria, we need to deal with each criterion separately and state what we need from it in order to evaluate the subject's identity. In the following we list all 27 criteria and explain their objectives. Because most of these criteria will be applied to the issuer's CP of the subject certificate, we will call the issuer the *issuer CA*.

5.2.1 Liability and Capability of the Subject (criterion 1)

In the case that the subject for whom we need to evaluate trustworthiness is a subordinate CA, this criterion assists us in determining whether the issuer CA had made sure that the subject is liable and capable as a certification provider. If this criterion is covered by the issuer of the subject's certificate then this will be recorded as a positive point in the evaluation of a subject's trustworthiness.

5.2.2 Allowance For RA to Issue Certificate (criterion 2)

The X.509 Internet draft [58] states that the RA has a number of functions to perform, but none are to do with issuing certificates. This criterion investigates the issuer CA's CP to check if it allows the RA to issue certificates, and if this is the case, the result will be a negative contribution to the subject's trustworthiness.

5.2.3 Financial Cover (criterion 3)

A business that offers any sort of financial cover will make a consumer more confident of its services. The Internet payment service "PayPal" offers financial insurance, called "Buyer Protection", of up to £500 [59]. If an issuer CA's CP permits financial responsibility for its certificates then the subject's certificate will also be covered. This criterion shows this in the formalisation and thus helps develop a positive image of the subject's trustworthiness.

5.2.4 National Law Enforcement (criterion 4)

A consumer will be more confident if national law covers any transactions. This has been adopted by many businesses, for instance Visa Inc., the world leader in electronic payments. It declares on its website that [60]:

The Rules will be governed by and construed under the laws of the State of California, excluding only its conflict of law provisions. Each party to the Visa site Rules hereby submits to the exclusive jurisdiction of the courts within the State of California, and waives any jurisdictional, venue, or inconvenient forum objections to such courts.

Criterion 4 examines whether or not national law covers any agreement; and if so, the subject's trust rating will be affected positively.

5.2.5 Dispute Reference (criterion 5)

Allowing for dispute referral or arbitration to settle any dispute arising between the issuer CA and the subject indicates that the issuer CA is honest and is confident of its service; accordingly, this shows that the issuer CA is trustworthy and its subjects inherit trustworthiness from it. The online marketplace, eBay, has affirmed this concern in its website thus [61]:

If a dispute arises between you and eBay, our goal is to provide you with a neutral and cost effective means of resolving the dispute quickly. Accordingly, you and eBay agree that we will resolve any claim or controversy at law or equity that arises out of this Agreement or our services (a "Claim") in accordance with one of the subsections below or as we and you otherwise agree in writing. Before resorting to these alternatives, we strongly encourage you to first contact us directly to seek a resolution by going to <http://pages.ebay.com/help/new/customer-support.html>. We will consider reasonable requests to resolve the dispute through alternative dispute resolution procedures, such as mediation or arbitration, as alternatives to litigation

Dispute reference will be represented in the formalisation by criterion 5.

5.2.6 Service Assessment (criterion 6)

Service assessment of the issuer CA is to see whether or not it is in compliance with what has been stated in the CP. This assessment is important for evaluating the organization's performance and it highlights areas of opportunity for improving its performance and complying with what is in the CP. This assessment is accomplished by doing a "compliance audit". The criterion checks if the compliance audit is carried out by an external auditor, and if so, this will suggest that the issuer CA is confident of its performance and that it has the desire to adopt recommendations regarding its performance. The subject whose identity we authenticate will gain positive reputation and its trustworthiness will be increased.

5.2.7 Frequency of Service Assessment (criterion 7)

If the issuer CA has outlined a periodical compliance audit, this will increase its trustworthiness adding to what has already been said in criterion 6; and it will have positive impact on the subject that we are authenticating. As an example, VeriSign Inc. conducts compliance audits at least annually [55].

5.2.8 Action on Deficiency (criterion 8)

To show the seriousness of the issuer CA in applying the two previous criteria, criterion 8 tests if there is any action taken as a result of irregularities in complying with the CP. If the issuer CA's CP contains this request then this will show that the issuer CA is keen to provide a quality service, and implies that its certificates are qualified. Consequently, the subscribers or subjects who have their certificates issued by such an issuer CA have gained trustworthy certificates which assists in making their trustworthiness positive. For example, VeriSign Inc. proposes the following action in the case of deficiencies [55]:

After receiving a report based on the Compliance Audit under CP § 2.7.6, the audited entity's Superior Entity shall contact the audited party to discuss any exceptions or deficiencies shown by the Compliance Audit. VeriSign shall also be entitled to discuss such exceptions or deficiencies with the audited party. The audited entity and the Superior Entity shall, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan. The audited entity's failure to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that VeriSign and the audited entity's Superior Entity reasonably believe pose an immediate threat to the security or integrity of the VTN, (a) VeriSign and/or the Superior Entity shall determine whether revocation and Compromise reporting are necessary under CP §§ 4.4.1.1, 4.4.15, (b) VeriSign and the Superior Entity shall be entitled to suspend services to the audited entity, and (c) if necessary, VeriSign and the

Superior Entity may terminate such services subject to CP § 4.9 and the terms of the audited entity's contract with its Superior Entity

5.2.9 Confidentiality of Personal Information (criterion 9)

Data protection law requests that companies process subscribers' personal information in a way that ensures privacy protection and that information must not be released without the prior consent of the subscribers, except when required by law. The UK Data Protection Act states this in the following paragraphs [62]:

Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless- (a) the other individual has consented to the disclosure of the information to the person making the request

When the issuer CA complies with its national data protection rules, subscriber confidence will increase, as stated in [57]:

In order to increase user confidence in electronic communication and electronic commerce, certification service-providers must observe data protection legislation and individual privacy;

Criterion 9 examines this requirement from the issuer CA's CP and based on that its trustworthiness will be evaluated.

5.2.10 Authentication of Organization Identity (criterion 10)

This criterion requests that the issuer CA authenticate the identity of an organization based on its publicity and popularity in the community where its issuer CA is located (evaluation of public reputation). One of the principles in "*Principles of Client Identification and Beneficial Ownership for the Securities Industry*" is called "*Know Your Client (KYC)*" and requests Securities Service Providers (SSPs) to obtain information about their clients, such as their circumstances and investment objectives,

in order to know them and to develop a profile of the client. The accumulated results for this process determine the client's risk profile (trustworthiness) [63]. Therefore, if the issuer CA has adopted this request, the authentication process for the subject (the organization) will show this through this criterion. As a result the confidence of the relying party will be increased and the organization's trustworthiness will be positive.

5.2.11 Authentication of Individual Identity (criterion 11)

In providing adequate proof of identification, criterion 11 requests that individuals present themselves personally to the authenticating authority, or possibly using other methods such as by videoconference [48] or a stamp from a licensed notary [64]. Appearing in person for the identification process will assist the authenticating authority to:

1. Know the subscriber well.
2. Making sure that the subscriber is the original requester for the certificate.
3. Ask for more proof in order to boost confidence.

As a solution to preventing identity theft, iSecuritas Inc. (iSI), a leading Internet security company, and Mail Boxes Etc. (MBE), the world's largest retail business, communications and postal service franchisor, have asked individuals to appear in the physical presence of official notaries public at MBE locations for proof of identity [65]. The subject's trustworthiness will be increased if its issuer CA asks for this type of identity authentication.

5.2.12 Informed Subject (criterion 12)

In the publication titled "*Principles of Consumer Protection for Electronic Commerce*", two out of eight principles relate to making consumers aware of their rights and obligations [66]:

Principle 1: *Consumers should be provided with clear and sufficient information to make an informed choice about whether and how to make a purchase.*

Principle 2: *“Vendors” should take reasonable steps to ensure that the consumer’s agreement to contract is fully informed and intentional.*

The subject is a consumer when requesting a certificate from an issuer CA. If subjects know their rights and obligations, this will lead to smooth operation without discontinuity, furthermore, it will make the issuer CA’s CP more effective at preventing any systemic deficiency. If the issuer CA’s CP requests this action, the criterion will show this, and the subject’s trustworthiness will be increased positively.

5.2.13 CRL Update Interval Time (criterion 13)

Issuing a CRL immediately after any certificate revocation will grant real-time certificate-status information and make the CRL mechanism more effective in stopping an attacker who has compromised a private key [67]. This criterion examines the interval time that is needed for an issuer CA to upload an updated CRL. With prompt CRL update, the trustworthiness of the issuer CA is likely to be positive and this will extend to cover the subject’s trustworthiness.

5.2.14 Validity Period of a CRL (criterion 14)

Periodic publishing of CRLs contributes to the level of trust of the CA because it assists a verifier in checking the validity of the subject’s certificate with a valid CRL, and to the reliability of the issuer CA’s services. The CA issues a new CRL on a regular periodic basis (e.g., hourly, daily, or weekly) [68], and the validity period of a CRL is specified by the administrator of the CA [69]. An issuer CA who complies with this request adds reliability to its certificates’ subject which increases their perceived trustworthiness.

5.2.15 Comprehensive Security Audit (criterion 15)

Security audit is a crucial tool for any organization because it enables the organization to retain its assets. Applying security audit will assist in accomplishing the following [70]:

- Investigating if there are any attacks from outside the organization.

- Preventing threats from inside the organization.
- Identifying areas that need more attention

Workplace violence (insider attack) has held first place for the last five years in a survey conducted by Pinkerton Inc. in 2003 [5]. Insider attackers will most likely succeed in extracting critical information because they know their organization's systems well [71]. The majority of these attackers are disgruntled employees [72]. By complying with this request, the issuer CA will be accredited positively and increase the relying party's confidence in its certificates' subject.

5.2.16 Security Audit Log Examination (criterion 16)

Through periodical review and analysis of audit logs, attacks will be discovered. As we stated in the previous section, attacks frequently come from inside an organization, and this type of attack is harder to discover; usually the only evidence for this type of crime is through the examination of audit logs [73]. Therefore, the trust assurance of the issuer CA will rise with compliance to this criterion, and consequently its certificates' subject will be affected positively.

5.2.17 Vulnerability Assessment (criterion 17)

We have discussed finding threats in the previous criteria (15 and 16) but examining the organization's systems for discovering vulnerabilities is considered a crucial assessment which must be accomplished by any organization. Identifying threats and vulnerabilities is a step toward making the organization's systems safer and more secure [74]. Vulnerability assessment is used to identify weaknesses in systems and assist the organization in correcting vulnerabilities so as not to leave vital organizational data exposed to malicious attacks. This criterion examines the issuer CA's CP to make sure this assessment is requested and if so, will increase its subject certificate's trustworthiness.

5.2.18 Archiving Procedure (criterion 18)

Criterion 18 asks that the archiving procedure include all events. An issuer CA who complies with this request demonstrates its accountability; moreover, this issuer CA will boost users' confidence and they will trust its certificates. Requirement 9 (Chapter 4) states the ultimate goal of archiving information which is for it to be used as evidence in legal proceedings. Therefore, a complete archive of events may be helpful in such a case.

5.2.19 Disaster Recovery Plan (criterion 19)

Resumption of operations quickly after a disaster will be based on a plan developed earlier, and if such a plan exists, demonstrates the reliability of the issuer CA. Preparation for disaster is not fully addressed by many companies: a survey of Fortune 1000 companies regarding disaster preparation shows that 22 percent did not meet the requirements for business continuity [6].

5.2.20 Trusted Roles (criterion 20)

To prevent any malicious behaviour, criterion 20 supports the assignment of separate duties for performing CA functions, known as trusted roles. Each person is assigned a specific task based on its functions such as day-to-day operation, administration of the CA, and management and audit of these tasks [54]. The basis of trust in the entire PKI comes from the fact that the functions performed are trusted; therefore, there should be a careful process when selecting who should get these roles. [75] states the process for selecting personnel who will serve in trusted roles:

Issuing CAs will conduct an appropriate investigation of all personnel who serve in Trusted Roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and the Issuing CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation will not serve or continue to serve in a Trusted Role.

5.2.21 Personnel Controls (criterion 21)

An organisation has to identify staff that will accomplish the entire procurement process and watch the subsequent steps to satisfy the need for continuity of its business and possible future procurement processes [20]. The most critical staff positions are the personnel who perform duties as CA or RA and they must be under control and should be assigned in writing or be bound by contract. Moreover, they must adhere to the terms and conditions of the position they are to fill [54]. When relying parties know how the issuer CA is managed, and knows what type of security controls that audit personnel functions, this will assist them to know the level of trust that they can place on the certificates issued by this issuer CA [20].

5.2.22 Subject Keys (criterion 22)

Criterion 22 does not allow an issuer CA to generate a subject's cryptographic keys so as to prevent the private key being compromised [76]. The private key should only be known to the key holder; therefore, this criterion requests that subjects generate their own key pairs.

5.2.23 Private Key Length (criterion 23)

Strong encryption is achieved with larger encryption keys; therefore, this criterion requires that any encryption key be at least 1024 bits; this key length has been specified as the minimum length for CAs [76].

5.2.24 Keys validity period (criterion 24)

Private and public keys for both CAs and subjects have to be renewed periodically because using keys for long periods makes them more susceptible to compromise and loss [77]. Therefore, the CP should set a defined period of validity for private and public keys.

5.2.25 CA Machine Security (criterion 25)

This criterion asks for strong security protection to be adopted to protect the CA system. Such protection includes:

- Not connecting CA systems to any data network.
- Prohibiting unauthorized access to CA systems.

These protections assist in guaranteeing the continuity of CA operations and in protecting the CA's private key which is the heart of CA trust. Compromise of this key results in loss of confidentiality, integrity and availability [78].

5.2.26 Maintaining Hardware and Software Integrity (criterion 26)

Checking the operation of hardware and software helps in discovering any deficiency and violation of security procedures; therefore, discovering these problems and fixing them increases the integrity of operation of the hardware and software; moreover, it is important for securing the systems [79].

5.2.27 Network Security (criterion 27)

A CP should define procedures for securing networks such as installation of devices to prevent network attacks, tampering, unauthorized access, and denial-of-service attacks.

5.3 Representing the Criteria in the Formalisation

We have defined the criteria and their meaning, and as we stated, we will use these criteria in the XML formalisation in order to perform comparisons with a subject's CP to define the level of trust that a relying party can place on the CP. This comparison will be accomplished by comparing the pre-defined value for the criteria with the subject's CP value. In this section we will mainly consider the process of representing the criteria in the XML formalisation and defining their values. Each criterion will be listed separately and its syntax in the representation will be developed.

5.3.1 Testing Liability and Capability of the Subject

The XML representation will present criterion 1 depending on the following parameters:

- Responsible participant: Certification Authority.
- Action to be accomplished: Making sure that subject is able to manage the subordinate CA.
- Constraint: In compliance with agreed CP.

The XML representation for criterion 1 in the terms of the specified parameters is given in the following:

```
<CertificationAuthority>
  <requirement>
    <checking>
      <capability of="subject" toManage="subordinate CA">
        <requirement>
          <withCompliance with="agreed CP"/>
        </requirement>
      </capability>
    </checking>
  </requirement>
</CertificationAuthority>
```

5.3.2 Prohibiting RA from Issuing Certificates

We have the following parameters that need to be presented in the XML formalisation:

- Responsible participant: Certification Authority.
- Action to be accomplished: Prohibiting RA from issuing certificates.

The following is the XML representation for criterion 2:

```
<RegistrationAuthority>
  <prohibition>
    <issue>
      <certificates to="subject"/>
    </issue>
  </prohibition>
</RegistrationAuthority>
```

5.3.3 Providing Financial Insurance

In criterion 3, we deal with the financial responsibility for any error, omission or inaccuracy whilst offering any PKI services. PKI services are offered by different participants, such as the CA, RA or subscriber. Under the section “Indemnification by Subscribers” in [80], issues that required financial responsibility have been listed:

- *Falsehood or misrepresentation of fact by the Subscriber on the Subscriber’s Certificate Application,*
- *Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,*
- *The Subscriber’s failure to protect the Subscriber’s private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber’s private key, or*
- *The Subscriber’s use of a name (including without limitation within a common name, domain name, or e- mail address) that infringes upon the Intellectual Property Rights of a third party.*

We distinguish the following parameters to be encoded in XML:

- Responsible participant: Participant.
- Action to be accomplished: as stated in [42], the XML formalisation should contain the following parameters,
 1. Declaring that it maintains an amount of insurance coverage for its liabilities to other participants.
 2. Declaring that it has resources to support operations and pay damages for potential liability.

The following lines illustrate our XML representation for the above:

```

<participant>
  <requirement>
    <declare>
      <financialResponsibility for="its liabilities" to="other participants"/>
      <assets to="support its operations and liabilities"/>
    </declare>
  </requirement>
</participant>

```

5.3.4 Enforcing National Law Superiority

A Certification Authority is responsible for making sure that its operation meets what has been defined in the CP [81]; therefore, the certification Authority should ensure that its national's law will govern any agreements. The parameters that describe criterion 4 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Ensure that national law governs any agreements.
- Constraint: Country law where CA is established; here we adopt the ISO standard country code as given in ISO 3166-1 [82].

Criterion 4 syntax in XML formalisation will be represented as:

```

<CertificationAuthority>
  <requirement>
    <ensure>
      <law ofCountry="ISO country name" governsAnyAgreement="true">
        <requirement>
          <sameCountry where="CA" isEstablished="true"/>
        </requirement>
      </law>
    </ensure>
  </requirement>
</CertificationAuthority>

```

5.3.5 Allowing For Arbitration in Cases of Dispute

Parameters for criterion 5 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Allow for arbitration to resolve disputes arising out of the CA's CP.

The XML representation of the above is:

```
<CertificationAuthority>
  <requirement>
    <allow>
      <arbitration to="resolve disputes arising out of its CP"/>
    </allow>
  </requirement>
</CertificationAuthority>
```

5.3.6 Performing Compliance Audit

The parameters involved in criterion 6 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Performing compliance audit.
- Constraint: Compliance audit should be carried out by an external auditor.

And the XML syntax for the above parameters is:

```
<CertificationAuthority>
  <requirement>
    <perform>
      <process of="compliance Audit">
        <requirement>
          <carryOut by="external auditor"/>
        </requirement>
      </process>
    </perform>
  </requirement>
</CertificationAuthority>
```

5.3.7 Performing Frequent Compliance Audit

Criterion 7 is a completion of criterion 6 and it sets a value for the number of times compliance the audit process is to be repeated. We require that the audit compliance process is performed at least annually whether there is a need or not; this requirement was identified in [83]:

The audit committee should monitor and review the internal audit activities. Where there is no internal audit function, the audit committee should consider annually whether there is a need for an internal audit function and make a recommendation to the board, and the reasons for

the absence of such a function should be explained in the relevant section of the annual report.

Criterion 7 XML representation:

```
<CertificationAuthority>
  <requirement>
    <run>
      <complianceAudit>
        <requirement>
          <annually atLeast="1"/>
        </requirement>
      </complianceAudit>
    </run>
  </requirement>
</CertificationAuthority>
```

5.3.8 Taking Action on Deficiency

Criterion 8 is the conclusion of the process that was started in criterion 6; we demand that action be taken against any non-compliance with the policy; [48] states that one of the reasons for the revocation of a subject’s certificate is when the subject violates its obligations. Therefore, the parameters for criterion 8 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Revoking the subject certificate.
- Constraint: Compliance audit showing that the subject operation does not comply with the CP.

The following is the XML used to represent criterion 8:

```
<CertificationAuthority>
  <requirement>
    <revoke>
      <subjectCertificate to="certificate revocation list">
        <requirement>
          <subjectOperation complyWithCP="false"/>
        </requirement>
      </subjectCertificate>
    </revoke>
  </requirement>
</CertificationAuthority>
```

5.3.9 Prohibiting A CA from Ever Disclosing Any Subject

Confidential Information

To insure that criterion 9 is handled correctly, the following parameters need to be considered in the XML representation:

- Responsible participant: Certification Authority.
- Action to be accomplished: No disclosure of a subject's confidential information.
- Constraint: Except with prior consent of the subject or when required by law.

The following is the XML representation of the criterion 9:

```
<CertificationAuthority>
  <prohibition>
    <discloseTo>
      <thirdParties any="confidential information" of="subject">
        <requirement>
          <except>
            <whenRequestedByLaw>true</whenRequestedByLaw>
            <whenConsentBySubject>true</whenConsentBySubject>
          </except>
        </requirement>
      </thirdParties>
    </discloseTo>
  </prohibition>
</CertificationAuthority>
```

5.3.10 Organization Authentication Should Include Organization's Reputation

Parameters for criterion 10 are covered in the following:

- Responsible participant: Registration Authority.
- Action to be accomplished: An authenticating organization must include its reputation.

The XML representation for the above parameters:

```

<RegistrationAuthority>
  <requirement>
    <authenticate>
      <organization include="its reputation"/>
    </authenticate>
  </requirement>
</RegistrationAuthority>

```

5.3.11 Authenticating the Identity of an Individual in Person

We have to represent in XML the following parameters :

- Responsible participant: Registration Authority.
- Action to be accomplished: RA must authenticate an individual's identity in person.

The syntax of criterion 11 in XML will be as follows:

```

<RegistrationAuthority>
  <requirement>
    <authenticate>
      <individual basedOn="its physical presence"/>
    </authenticate>
  </requirement>
</RegistrationAuthority>

```

5.3.12 Informing the Subject of Rights and Obligations

We have the following parameters:

- Responsible participant: Certification Authority.
- Action to be accomplished: Ensure that subjects are aware of their rights and obligations.

And here is the XML representation for criterion 12's parameters:

```

<CertificationAuthority>
  <requirement>
    <insure>
      <subject isAwareOf="its respective rights and obligations"/>
    </insure>
  </requirement>
</CertificationAuthority>

```

5.3.13 Updating the CRL Immediately on Certificate Revocation

We assign criterion 13's parameter the value of "within one hour"; which indicates that we ask for an update of the CRL within one hour of every certificate revocation. Immediate updating of the CRL will provide more assurance [84]. This value has been selected in the DutchGrid CP [52]:

- Responsible participant: Certification Authority.
- Action to be accomplished: Updating CRL after every certificate revocation.
- Constraint: Interval time must be within one hour since revocation.

Criterion 13's XML representation is:

```
<CertificationAuthority>
  <requirement>
    <update>
      <CRL after="every certificate revocation">
        <requirement>
          <updateIntervalTime withIn="1 hour"/>
        </requirement>
      </CRL>
    </update>
  </requirement>
</CertificationAuthority>
```

5.3.14 Issuing Frequent CRLs

Publishing complete base CRLs frequently would lead to high network traffic due to the frequent downloading of the updated CRL by clients. On the other hand, if the CRL is published after a long interval, this will affect the validity of the CRL as a result of it containing out-of-date information. Using delta CRLs, produces a smaller file, and solves these problems by showing revoked certificates until the next update of the base CRL. Delta CRLs can be published at short intervals such as once an hour (this is covered in criterion 13) [34]; and the base CRL can be published at long intervals. In this criterion we define the value of the interval time for frequent base CRL update; and we have assigned the value "30 days" for criterion 14. The following are the parameters for this criterion:

- Responsible participant: Certification Authority.

- Action to be accomplished: Updating CRL frequently.
- Constraint: Interval time must be equal to 30 days.

Criterion 14's XML representation is:

```

<CertificationAuthority>
  <requirement>
    <publish>
      <CRL>
        <requirement>
          <intervalTime withIn="30 days"/>
        </requirement>
      </CRL>
    </publish>
  </requirement>
</CertificationAuthority>

```

5.3.15 Performing Comprehensive Security Audit

With regards to the following documents:

- Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements [85].
- Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework [42].
- DOE Grids Certificate Policy and Certification Practice Statement [86].
- VeriSign Certification Practice Statement [80].
- CESNET CA Certificate Practice Statement [87].
- Certificate Practice Statement for The Commonwealth of Pennsylvania Department of Environmental Protection [88].
- DutchGrid and NIKHEF - Medium-security X.509 Certification Authority - Certification Policy and Practice Statement [52].

We have extracted a list of events that must be recorded during the security audit process:

- All boots of the PKI system.
- All access attempts to PKI system.
- All PKI system failures.

- CA key generation.
- CA key storage.
- CA key backup.
- CA key archival.
- CA key recovery.
- CA key destruction.
- CA and subject certificate generation requests.
- CA and subject certificate renewal requests.
- CA and subject certificate re-key requests.
- CA and subject certificate revocation requests.
- Issuance of certificates.
- Other certificate requests made to the PKI system which include:
 - o Status change requests
 - o Status requests
 - o Responses
- PKI and security system actions performed by CA personnel.
- Identity verification procedures.

Therefore, the parameters of the criterion 15 are the following:

- Responsible participant: Certification Authority.
- Action to be accomplished: Doing comprehensive security audit.

The XML representation will be as the following:

```

<CertificationAuthority>
  <requirement>
    <do>
      <securirtyAudit>
        <requirement>
          <allBootsOfThePKISystem>true</allBootsOfThePKISystem>
          <allAccessAttemptsToPKISystem>true</allAccessAttemptsToPKISystem>
          <allPKISystemFailures>true</allPKISystemFailures>
          <CAkeyGeneration>true</CAkeyGeneration>
          <CAkeyStorage>true</CAkeyStorage>
          <CAkeyBackup>true</CAkeyBackup>
          <CAkeyArchival>true</CAkeyArchival>
          <CAkeyRecovery>true</CAkeyRecovery>
          <CAkeyDestruction>true</CAkeyDestruction>
          <CAandSubjectCertificate>
            <generationRequests>true</generationRequests>
          </CAandSubjectCertificate>
        </requirement>
      </securirtyAudit>
    </do>
  </requirement>
</CertificationAuthority>

```

```

        <renewalRequests>true</renewalRequests>
        <re-keyRequests>true</re-keyRequests>
        <revocationRequests>true</revocationRequests>
    </CAandSubjectCertificate>
    <issuanceOfCertificates>true</issuanceOfCertificates>
    <certificateRequests>
        <ofStatusChange>true</ofStatusChange>
        <ofStatus>true</ofStatus>
        <responses>true</responses>
    </certificateRequests>
    <PKIandSecuritySystemActions>
        <performedByCApersonnel>true</performedByCApersonnel>
    </PKIandSecuritySystemActions>
    <identityVerificationProcedures>true</identityVerificationProcedures>
</requirement>
</securirtyAudit>
</do>
</requirement>
</CertificationAuthority>

```

5.3.16 Examining Audit Logs Frequently

System security audit should not be done only once but be a regular task because the system changes every day and thus its security structures and requirements also change [89]. We have assigned the value “at least weekly” for criterion 16; and the parameters are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Examine security audit logs.
- Constraint: Examination of audit logs should be performed at least weekly.

The XML representation for the above parameters is:

```

<CertificationAuthority>
  <requirement>
    <examine>
      <auditLogs>
        <requirement>
          <frequent atLeast="weekly"/>
        </requirement>
      </auditLogs>
    </examine>
  </requirement>
</CertificationAuthority>

```

5.3.17 Performing Vulnerability Assessment

Parameters which represent criterion 17 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Perform vulnerability assessment.

And the XML syntax is:

```

<CertificationAuthority>
  <requirement>
    <execute>
      <process of="vulnerability assessments"/>
    </execute>
  </requirement>
</CertificationAuthority>
```

5.3.18 Providing Extensive Archiving

With regard to the following CPs:

- National Computational Science Alliance Certificate Policy [90].
- Certificate Policy and Certification Practice Statement [91].
- Certificate Policy and Certification Practice Statement CNRS/CNRS-Projets/Datagrid-fr [92].
- Model Certificate Policy [93].
- VeriSign Trust Network, Certificate Policies [55]

We get the following events that need to be archived:

- Certificate request application
- Documentation supporting certificate applications
- All computer security audit data
- Certificate revocation application
- Certificate re-key application
- Certificate renewal application data
- Issued Certificates
- Issued CRLs or certificate status records
- All correspondence between the CA and subcontractors and subscribers.

The archive that contains the above events needs to be retained for a certain time after the expiration of the key material. We ask that data be retained for five years [94]. Thus, according to the above events, the following are the parameters:

- Responsible participant: Certification Authority.
- Action to be accomplished: Provide an extensive Archiving.
- Constraint: Archived data should be retained for at least five years.

The XML syntax for criterion 18 is:

```
<CertificationAuthority>
<requirement>
<provide>
  <archiving>
    <requirement>
      <certificateRequestApplication>true</certificateRequestApplication>
      <documentationSupportingCertificateApplications>true</documentationSupportingCertificateApplications>
      <allComputerSecurityAuditData>true</allComputerSecurityAuditData>
      <certificateRevocationApplication>true</certificateRevocationApplication>
      <certificateRe-keyApplication>true</certificateRe-keyApplication>
      <certificateRenewalApplication>true</certificateRenewalApplication>
      <issuedCertificates>true</issuedCertificates>
      <issuedCRLsORcertificateStatusRecords>true</issuedCRLsORcertificateStatusRecords>
      <allcorrespondence>
        <betweenTheCAandSubcontractors>true</betweenTheCAandSubcontractors>
        <betweenTheCAandSubscribers>true</betweenTheCAandSubscribers>
      </allcorrespondence>
      <retentionPeriod>
        <atLeast InYears="5"/>
      </retentionPeriod>
    </requirement>
  </archiving>
</provide>
</requirement>
</CertificationAuthority>
```

5.3.19 Establishing a Disaster Recovery Plan

The parameters that represent criterion 19 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Establish a disaster recovery plan for resuming operations immediately after a disaster.

The following is its XML syntax:

```

<CertificationAuthority>
  <requirement>
    <establish>
      <plan of="surviving after the disaster"/>
    </establish>
  </requirement>
</CertificationAuthority>

```

5.3.20 Supporting Trusted Roles

The trusted roles that we ask a CA to support are the same as the ones identified in [85] which are:

- Security Officers
- Registration Officers
- System Administrators
- System Operators
- System Auditors

Therefore, parameters will present the above data as in the following:

- Responsible participant: Certification Authority.
- Action to be accomplished: Support at least the following trusted roles:
 - Security Officers
 - Registration Officers
 - System Administrators
 - System Operators
 - System Auditors

The XML representation is:

```

<CertificationAuthority>
  <requirement>
    <support>
      <trustedRoles>
        <requirement>
          <securityOfficers>true</securityOfficers>
          <registrationOfficers>true</registrationOfficers>
          <syemAdministrators>true</syemAdministrators>
          <systemOperators>true</systemOperators>
          <systemAuditors>true</systemAuditors>
        </requirement>
      </trustedRoles>
    </support>
  </requirement>
</CertificationAuthority>

```

5.3.21 Personnel Controls

We use the following CPs to identify the controls that we ask to be applied:

- Certificate Policy for the State of Washington Public Key Infrastructure [64].
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [95].
- Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, RFC 3647 [42].

And in the following the parameters for criterion 21:

- Responsible participant: Certification Authority.
- Action to be accomplished: Ensure that all personnel performing duties with respect to the operation of a CA or RA are controlled by:
 - ☐ Checking personnel background:
 - ☐ Qualifications
 - ☐ Experience
 - ☐ Government clearances
 - ☐ Providing personnel with the requisite training
 - ☐ Providing personnel with refresher training and updates
 - ☐ Sanctioning personnel for unauthorized actions
 - ☐ Providing personnel with documentation relevant to their job functions

These parameters will be represented in XML as:

```

<CertificationAuthority>
  <requirement>
    <assure>
      <allPersonnelControlled>
        <requirement>
          <backgroundChecked>
            <qualifications>true</qualifications>
            <experience>true</experience>
            <governmentClearances>true</governmentClearances>
          </backgroundChecked>
          <providingWithTaining>true</providingWithTaining>
          <povidingWithRefresherTaining>true</povidingWithRefresherTaining>
          <sanctioningForUnauthorizedActions>true</sanctioningForUnauthorizedActions>
          <providingWithDocumentation>true</providingWithDocumentation>
        </requirement>
      </allPersonnelControlled>
    </assure>
  </requirement>
</CertificationAuthority>

```

5.3.22 Subject Generates Its Own Key Pairs

Parameters of criterion 22 are shown in the following:

- Responsible participant: Subject.
- Action to be accomplished: Generating its public and private key pair.

And the XML representation is:

```

<subject>
  <requirement>
    <generate>
      <itsKeys>true</itsKeys>
    </generate>
  </requirement>
</subject>

```

5.3.23 Minimum Length of the Private Key

Parameters that describe criterion 23 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Ensure that the minimum length of the private key must not be less than 1024 bits.

The XML representation of the above parameters is:

```

<CertificationAuthority>
  <requirement>
    <makeSure>
      <minimumLength of="private key" isInBits="1024"/>
    </makeSure>
  </requirement>
</CertificationAuthority>

```

5.3.24 Key Validity Periods

We will follow what has been defined in [76] which states that CA key usage periods should not exceed twenty years and subject keys will last one year maximum. The parameters that carry out these standards will be in the following:

- Responsible participant: Certification Authority.
- Action to be accomplished: Should not issue certificates to
 - CA : with validity periods more than 20 years
 - Subject : with validity periods more than 1 year

Criterion 24's syntax in XML will be:

```

<CertificationAuthority>
  <prohibition>
    <create>
      <CAcertificateValidityPeriods moreThanInYears="20"/>
      <subjectCertificateValidityPeriods moreThanInYear="1"/>
    </create>
  </prohibition>
</CertificationAuthority>

```

5.3.25 Protection of the CA Machine against Unauthorized Access

After we studied the following CPs:

- UK e-Science Certification Authority Certificate Policy and Certification Practices Statement [96].
- VeriSign Trust Network, Certificate Policies [55].
- DOE Grids Certificate Policy And Certification Practice Statement [86].

We identified the following parameters for criterion 25:

- Responsible participant: Certification Authority.
- Action to be accomplished: Secure CA machine by applying the following actions:
 - CA system separated from any network
 - Unauthorized access to CA system prohibited
 - Operating systems are maintained at a high level of security by applying all recommended and applicable security patches
 - Limiting access to CA system by reducing services to the bare minimum

The XML representation of the above parameters is:

```

<CertificationAuthority>
  <requirement>
    <secure>
      <CAmachine>
        <requirement>
          <disconnectFromNetwork>true</disconnectFromNetwork>
          <prohibitUnauthorizedAccess>true</prohibitUnauthorizedAccess>
          <updatingOSwithSecurityPatches>true</updatingOSwithSecurityPatches>
          <limitAccess>true</limitAccess>
        </requirement>
      </CAmachine>
    </secure>
  </requirement>
</CertificationAuthority>

```

5.3.26 Checking the Integrity of the Hardware and Software

The following CPs were used to identified the parameters:

- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) [97].
- VeriSign Trust Network, Certificate Policies [55].
- Certificate Policy, Digital Signature Medium Strength Soft Certificates [54].

We need to represent the following parameters in XML:

- Responsible participant: Certification Authority.

- Action to be accomplished: Examine the integrity of the hardware and software by performing the following:
 - Monitoring the CA system by documenting and controlling any:
 - ☐ Configuration
 - ☐ Modifications
 - ☐ Upgrades
 - Detecting unauthorized modification to the CA software or configuration
 - Checking the integrity of the CA software at least weekly

And the following is the XML representation:

```

<CertificationAuthority>
  <requirement>
    <examining>
      <integrityOfHardwareAndSoftwareBy>
        <requirement>
          <documentedAndControlledAny>
            <configuration>true</configuration>
            <modifications>true</modifications>
            <upgrades>true</upgrades>
          </documentedAndControlledAny>
          <detectingUnauthorizedModification>true</detectingUnauthorizedModification>
          <checkingSoftwareIntegrity>
            <atLeast inDays="7"/>
          </checkingSoftwareIntegrity>
        </requirement>
      </integrityOfHardwareAndSoftwareBy>
    </examining>
  </requirement>
</CertificationAuthority>

```

5.3.27 Securing Networks

In the following documents, network security controls issues are discussed highlighting controls to be used to secure a network:

- BT Certification Practice Statement [98]
- Certificate Practice Statement for The Commonwealth of Pennsylvania Department of Environmental Protection [88].

- NIIF Certification Authority, Certification Practice Statement (CPS) [99].
- Implementing Network Security Controls for Intrusion Prevention [100].

These controls include the following:

- Installing firewalls.
- Protecting communications through the use of encryption and digital signatures.
- Placing Access Control Lists (ACLs) on all network devices.

Therefore, parameters that represent criterion 27 are:

- Responsible participant: Certification Authority.
- Action to be accomplished: Securing networks by using:
 - Firewalls
 - Encryption and digital signatures
 - Access Control Lists (ACLs)

The XML syntax for above parameters is:

```
<CertificationAuthority>
  <requirement>
    <securing>
      <networks>
        <requirement>
          <firewalls>true</firewalls>
          <encryptionAndDigitalSignatures>true</encryptionAndDigitalSignatures>
          <ACLs>true</ACLs>
        </requirement>
      </networks>
    </securing>
  </requirement>
</CertificationAuthority>
```

5.4 Measurable Criteria

We suggest using a numerical evaluation system to make the final decision about the suitability of a subject's CP with the defined criteria. We could base our decision upon the defined criteria without using a numerical evaluation system, but we will end up with a decision that shows the number of similar criteria and the number those that are dissimilar. Using a numerical rating assists us to give a value showing the overall

relevance of the compared criteria. First we need to develop a scoring system to be used as quantitative weighting of the criteria.

5.4.1 Scoring System

Table 5-1 shows all criteria and their weighting. In the weighting column, there are four sub-weighting columns. The "Obligation Title" assigns equivalent weight to the subject obligation title if the subject's criterion has the same obligation title as the criterion, such as "requirement". The "Action" column specifies the weight for the action part of the criterion, and the "Constraint" column does the same for the constraint part (see the examples later in this chapter).

Criterion	Weighting			Criterion	Weighting			Criterion	Weighting		
	Obligation Title	Action	Constraint		Obligation Title	Action	Constraint		Obligation Title	Action	Constraint
1	1	1	1	10	1	1	NA	19	1	1	NA
2	1	1	NA	11	1	1	NA	20	1	1	5
3	1	2	NA	12	1	1	NA	21	1	1	7
4	1	1	1	13	1	1	1	22	1	1	NA
5	1	1	NA	14	1	1	1	23	1	1	NA
6	1	1	1	15	1	1	19	24	1	2	NA
7	1	1	1	16	1	1	1	25	1	1	4
8	1	1	1	17	1	1	NA	26	1	1	5
9	1	1	2	18	1	1	11	27	1	1	3

Table 5-1 The Scoring System

We use a simple additive module using weights that are assigned in Table 5-1 to produce the final numeric result. The final numeric result equals the sum of the criterion weights. The following equation illustrates this point:

$$ND = \sum_{i=1}^{27} Cw_i, \quad (1)$$

Where ND represents the Numeric Decision value, Cw is the criterion weight which is the sum of the weights of "Obligation Title" "Action" and "Constraint" columns. The value of i represents the number of the criteria.

To illustrate equation (1) consider the following example:

Criterion 7 deals with the issue of compliance audit and the following is its syntax:

```

<CertificationAuthority>
  <requirement>
    <run>
      <complianceAudit>
        <requirement>
          <annually atLeast="1"/>
        </requirement>
      </complianceAudit>
    </run>
  </requirement>
</CertificationAuthority>

```

And let us assume that the subject that we evaluate has its certificate is managed by the following CP:

Citizen & Commerce Certificate Policy [101],

The subject CP states the following regarding the compliance audit procedure:

This policy requires successful compliance audit prior to applying for provisional or approved status. The compliance auditor must be organizationally independent from the owner of the CA and qualified to audit CA processes. To maintain approved status, a CA must repeat the compliance audit process at least every three years.

The XML representation for the above subject CP passage is:

```
<CertificationAuthority>
  <requirement>
    <run>
      <complianceAudit>
        <requirement>
          <annually atLeast="0"/>
        </requirement>
      </complianceAudit>
    </run>
  </requirement>
</CertificationAuthority>
```

When we compare the two representations we find that the subject CP requires the compliance audit to be repeated at least every three years but in criterion 7 this process must be accomplished at least once every year. Therefore, according to Table 5-1 the weight for the subject criterion is 2 because it has not dealt with this issue properly according to identified criterion. The subject criterion value will be added with other criteria values to form the ND value.

The State of Illinois has specified that the frequency time for CRL updates is at least 24 hours [53], but in the relevant criterion (number 14) we assign the value of 30 days. The following is an XML representation of the State of Illinois' CP:

```
<CertificationAuthority>
  <requirement>
    <publish>
      <CRL>
        <requirement>
          <intervalTime withIn="24 hours"/>
        </requirement>
      </CRL>
    </publish>
  </requirement>
</CertificationAuthority>
```

And this is criterion 14's XML representation:

```
<CertificationAuthority>
  <requirement>
    <publish>
      <CRL>
        <requirement>
          <intervalTime withIn="30 days"/>
        </requirement>
      </CRL>
    </publish>
  </requirement>
</CertificationAuthority>
```

In this case, the weight that will be assigned for subject criterion is 3 because its interval time for frequency update is smaller than the interval time of criterion 14; this means that recently updated CRLs are available to the relying party. Although the smaller interval time causes more network traffic as we stated above, here we just compare the two values and their results.

5.5 Comparison Result

After assigning all the subject criteria weights, we can use equation 1 to get the value of the ND. This value is used to measure the trustworthiness of the target based upon what has been defined in the criteria. We have to bear in mind that “trusts” can only be interpreted in the context of the particular task or service which the relying party is expecting the subject to provide. In that sense, the result of the comparison will depend upon a part of each policy only. Taking account of this, we may consider the value of ND as yielding one of three situations:

1. No overlap.
2. Absolute overlap.
3. Partial overlap.

5.5.1 No Overlap

In this case the value of ND is 0 and this means that the subject’s CP and the identified criteria are disjoint. This leads us to conclude that no trust path exists. This situation is shown by the Figure 5-1:

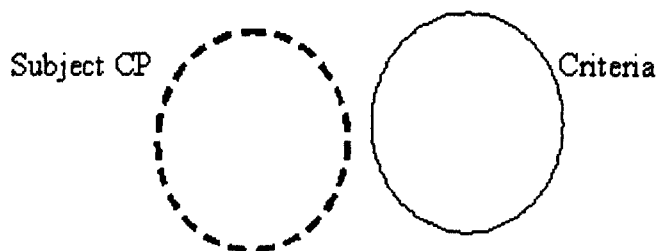


Figure 5-1 No Overlap Case

5.5.2 Absolute Overlap

The relevant sections of the criteria and the subject's CP impose the same constraints on the certificates within the two domains. Thus, every obligation, prohibition, etc. in criteria is matched by a corresponding obligation, prohibition in the subject's CP, therefore, the value of the ND is 120 (the result of adding the weights in the columns: "Obligation Title", "Action" and "Constraint"). In this case, the relying party should trust certificates in the subject domain. This is represented in Figure 5-2, where criteria are represented by the solid line and subject by the dashed line:

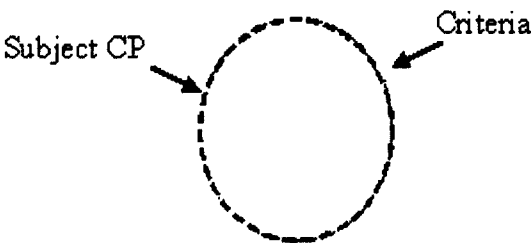


Figure 5-2 Absolute Overlap Case

5.5.3 Partial Overlap

Partial overlap means that the criteria and subject's CP have an intersection between them. Figure 5-3 shows this case:

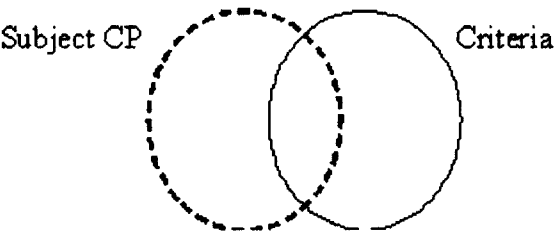


Figure 5-3 Partial Overlap Case

Here the subject's CP intersects with the criteria, indicating that the two policies have some aspects in common, but each has constraints which do not apply to the other policy. The subject's criteria have not covered all aspects adequately which cause the

value of ND to be less than 120; therefore, relying parties can trust certain activities but not others.

5.6 Acceptable Case

The cases above are decisions about the compatibility of a subject's CP with the criteria. The case that complies with the requirement of compatibility: absolute overlap. As we are trying to authenticate a certificate issued by an unknown CA, we accept only the absolute overlap case to be the authenticator for the subject's certificate. Our decision is based on all the criteria being covered by the subject's CP for the following reasons:

1. The criteria were developed by assessing several certification authorities' CPs, and the assessment process considered the making of a good balance between technical and legal requirements.
2. The assessment process extracted the criteria from the participating CPs as they have a significant role in defining the obligations.
3. The DTI requirements for issuing qualified certificates were applied to the candidate criteria on completion of the assessment process which produced the 27 criteria.

Based on these reasons, the 27 criteria are crucial for stating the trustworthiness of a subject's certificate and therefore the absolute overlap case is the only acceptable cases.

5.7 Conclusion

In this chapter we worked further to shape the criteria we developed in the previous chapter. First, we stressed the importance of these in making a decision about a subject's trustworthiness by presenting the semantic of these criteria. As we had defined the overall objectives of the criteria, this process showed the underlying objectives of each criterion. Then, we described the XML representation of each criterion with the defined values which will assist us in doing the comparison. Finally, we presented our system for weighting each criterion according to the results of the

comparison process and introduced the four cases that describe the trustworthiness of a subject and defined the acceptable cases.

CHAPTER 6

COMPARISON OF CRITERIA WITH REQUIREMENTS

6.1 Introduction

The criteria worked out in Chapter 5 must be examined, in order to determine if they are in conformity with requirements imposed by the international community. An example of such a requirement is the Commission of the United Nations' law of international trade (UNCITRAL Model Law on Electronic Signatures). In this chapter, we examine the criteria, demonstrating how they handle the articles identified by this law.

6.2 UNCITRAL Model Law on Electronic Signatures

The UNCITRAL Model Law on Electronic Signatures[102], hereafter referred to as UNCITRAL law, was created by the United Nations to further the progressive harmonization and the unification of international trade law and in this respect considers the interests of everyone, in particular those in developing countries so as to guarantee extensive development of international trade. In addition, it aims to ensure legal security in the context of the broadest possible use of automated data processing in international trade [102].

By using the UNCITRAL law to examine the criteria we have developed, we aim to see the convergence of the criteria and the degree of their effectiveness with respect to what it has been defined in the UNCITRAL law. The UNCITRAL law contains 12 articles:

Article 1. Sphere of application

Article 2. Definitions

Article 3. Equal treatment of signature technologies

Article 4. Interpretation

Article 5. Variation by agreement

Article 6. Compliance with a requirement for a signature

Article 7. Satisfaction of article 6

Article 8. Conduct of the signatory

Article 9. Conduct of the certification service provider

Article 10. Trustworthiness

Article 11. Conduct of the relying party

Article 12. Recognition of foreign certificates and electronic signatures

All UNCITRAL's articles are listed in Appendix C.

It is important to mention the following points:

1. Digital signature has as one of its functions validation of the identity of a user [103], which is the same as the scope of our criteria; therefore, we use the UNCITRAL law to examine the criteria. Moreover, UNCITRAL law in Article 2 states the function of digital signature as follows:

"Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

2. Some of the articles could not be used to test the criteria because they are articles which provide an interpretation and a description of the UNCITRAL law. The articles that will be used for examining our criteria are:

Article 6. Compliance with a requirement for a signature

Article 8. Conduct of the signatory

Article 9. Conduct of the certification service provider

Article 10. Trustworthiness

3. There are a number of paragraphs or factors in the articles that are either considered as fundamental functions or are out of the scope of the criteria. In this case we will define their relation to the criteria or their pre-implementation in the CP.
4. There are a number of criteria applicable to more than one article; we will relate the criteria to the most relevant article.

6.2.1 Article 6. Compliance with a Requirement for a Signature

1. *Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

Paragraph 1 specifies the condition under which a digital signature has the same legitimacy as a handwritten signature which leads us to consider whether a digital signature is as reliable as a handwritten signature. This case is a special rule applied only in the case of digital signature; it is not applicable in the case of certificates; so is out of the scope of our criteria.

2. *Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.*

Paragraph 2 applies only in the case of a digital signature, and therefore it is irrelevant to the criteria's scope.

3. *An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: (a) The*

signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

Paragraph 1 (a) is relevant when a subject requests a certificate, the RA validates documents presented by subject and makes sure that they belong to the subject. The paragraph refers to a fundamental task that is an early stage of the certificate issuing process, thus paragraph 1 (a) is not covered by our criteria.

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

What has been said about factor (a) is also true for this.

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

In the case of the certificate, the CA public key and the CP assists in detecting any alteration, in other words, they work as a validator for the certificate. This technique is considered an essential function of PKI, and the criteria therefore do not cover this factor.

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

A certificate validates a subject's identity, and in the case where there is any suspicious behaviour the owner of the certificate will easily discover it and revoke the certificate [104]. Our criteria concern the repository of the revoked certificates, CRL, and defined the interval time that is needed for an updated CRL and the validity period of the CRL.

4. *Paragraph 3 does not limit the ability of any person: (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or*

Increasing reliability of the certificate is the main goal of a CA and this is achieved through compliance with the CP. There is no requirement on a CA to define or use

anything that leads to an increase in the reliability of a certificate [105]. Our criteria in total examine a number of issues that are defined in the subject CP which yield an evaluation of the reliability of the subject certificate.

(b) To adduce evidence of the non-reliability of an electronic signature.

This mechanism is guaranteed by the CP and allows for revocation or suspension of a certificate if there is any doubt regarding its validity.

6.2.2 Article 8. Conduct of the Signatory

1. *Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;*

Two criteria examine the subject CP practices for avoiding unauthorized use. Criterion 9 obliges a CA not to disclose subject certificate-related data to any third party, and criterion 22 requests a subject to generate its own key pair to avoid key compromise and unauthorized use.

(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or

Factor (b) is considered one of the core functions of PKI [106], and it is an obligation on a subject to notify the CA immediately there is any compromise. The CA provides more information about carrying out this function in the CP in the section “Certificate Suspension and Revocation”. If the CA’s private key is compromised or suspected of being compromised, the CA shall inform subjects and relying parties, and terminate the certificates and produce a CRL.

(ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

The CP contains different security practices that help discover any violation in using certificates and that will result in revocation or suspension of the violated certificate.

(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

Certificates are issued by the CA after it validates the subject data, and this remains true through the lifecycle of the certificate. In other words, if the data related to the certificate becomes inaccurate, the CA immediately suspends the subject certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

In the case of a certificate, this request is satisfied when the subject accepts the provisions of the contract before the issue of the certificate [107]; criterion 12 request that subjects should be fully informed of their rights and obligations.

6.2.3 Article 9. Conduct of the Certification Service Provider

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: (a) Act in accordance with representations made by it with respect to its policies and practices;

Criterion 6 shows if the CA is in compliance with what has been stated in the CP through performing an assessment called a “compliance audit”.

(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

Our criteria meet the contents of paragraph 1 (b) with a number of criteria that examine the CA’s policies and practices which it operates throughout the life cycle of its certificates to ensure accuracy and reliability. These criteria are:

- Criterion 1 checks the liability and capability of the future CA, known as a subordinate CA, in performing all the controls and checks detailed in the CP.
- Criterion 2 restricts the issuing of the certificate only to the CA and prohibits an RA from doing this.
- Criterion 15 requests a comprehensive security audit.
- Criterion 16 asks for periodical review and analysis of audit logs.
- Criterion 17 requires vulnerability assessment.
- Criterion 19 asks for a disaster recovery plan.
- Criterion 22 restricts the issuing of subject keys to the subject.
- Criterion 23 defines a minimum length for the subject's private key.
- Criterion 24 specifies the validity period for private and public keys.
- Criterion 25 sets rules for protecting the CA system.
- Criterion 27 defines procedures for securing networks.

(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate: (i) The identity of the certification service provider;

The identity of the CA is readily determined from the certificates that it issues and from its CP.

(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

Basically, a certificate will not be issued if the RA came across any deficiency related to the subject data.

(iii) That signature creation data were valid at or before the time when the certificate was issued;

The previous sub-paragraph clarification is also applicable here.

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i) The method used to identify the signatory;

This request is specified in the CA's CP, and our criteria accept two identification methods. First to identify the organization, is covered by criterion 10 and the second specifies the identification method for the individual subject and is covered in criterion 11.

(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;

Any limitation on the use of the subject certificate is easily worked out from the certificate. The criteria will apply if the certificate is not restricted to purposes which the CA has specified.

(iii) That the signature creation data are valid and have not been compromised;

The RA function is one of the trusted roles, and it checks the subject's data to make sure of its validity before a CA issues the subject's certificate.

(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;

The CA's CP declares explicitly any limitation or the extent of the CA's liability.

(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law;

As we stated in paragraph 6.2.2 1 (b) above, this mechanism is essential to prevent malicious attacks; thus all CPs explain in details how a subject carries this out.

(vi) Whether a timely revocation service is offered;

A timely revocation service is offered by the PKI, and it is easy to check if this mechanism is offered by a CA by looking at its CP.

(e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;

Our criteria examine the availability of a timely revocation service using two aspects of the CRL. The first is the interval time needed for a CA to revoke a certificate and upload an updated version of the CRL (Criterion 13). Second, criterion 14 examines the validity period of the CRL.

(f) Utilize trustworthy systems, procedures and human resources in performing its services.

The most important part of a CA is the personnel who perform the duties of CA or RA. Our criteria ensure the trustworthiness of a CA's personnel by examining two constraints; first, if the subject CP provides a separation of duties for critical CA functions known as "trusted roles"; this constraint is covered by criterion 20. Second, to check if personnel controls are adopted in the subject's CP and this constraint is met by criterion 21.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Criterion 4 considers National law as covering any agreement, and this means if the CA's CP does not cover this requirement, our criteria guarantee that National law complies at least with paragraph 2.

6.2.4 Article 10. Trustworthiness

For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors: (a) Financial and human resources, including existence of assets;

The criteria meet this requirement through 3 which requests financial cover.

(b) Quality of hardware and software systems;

This requirement is satisfied by criterion 26 with the aim of maintaining hardware and software integrity.

(c) Procedures for processing of certificates and applications for certificates and retention of records;

Procedures relating to certificates are fully described in the CA's CP, and these procedures are tested and audited by the CA to grantee their integrity. Our criteria are concerned with evidence in the case of legal disputes i.e. data archiving. Criterion 18 deals with this requirement.

(d) Availability of information to signatories identified in certificates and to potential relying parties;

Information that addresses issues related to certificates is available to subjects and relying parties; this is outlined in the CP under the section titled "Publication and Repository".

(e) Regularity and extent of audit by an independent body;

Criterion 7 defines the frequency of compliance audit carried out by an external body, and this constraint is specified in criterion 6 which is covered under article 9, paragraph 1 (a).

(f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

The result of the compliance test conducted by an external body will be declared according to the CP section titled "Communication of results". Our criteria require that when there are irregularities in complying with the CP an action should be taken: criterion 8.

We have used the UNCITRAL law to examine the developed criteria and to summarize this assessment, table 6-1 shows the correspondence between the developed criteria and the UNCITRAL law articles:

Developed criteria	UNCITRAL law articles
Criterion 1	Article 9, paragraph 1 (b)
Criterion 2	Article 9, paragraph 1 (b)
Criterion 3	Article 10 (a)
Criterion 4	Article 9, paragraph 2
Criterion 5	
Criterion 6	Article 9, paragraph 1
Criterion 7	Article 10 (e)
Criterion 8	Article 10 (f)
Criterion 9	Article 8, paragraph 1
Criterion 10	Article 9, paragraph 1 (d)
Criterion 11	Article 9, paragraph 1 (d)
Criterion 12	Article 8, paragraph 2
Criterion 13	Article 9, paragraph 1 (e)
Criterion 14	Article 9, paragraph 1 (e)
Criterion 15	Article 9, paragraph 1 (b)
Criterion 16	Article 9, paragraph 1 (b)
Criterion 17	Article 9, paragraph 1 (b)
Criterion 18	Article 10 (c)
Criterion 19	Article 9, paragraph 1 (b)
Criterion 20	Article 9, paragraph 1 (f)
Criterion 21	Article 9, paragraph 1 (f)
Criterion 22	Article 8, paragraph 1
Criterion 23	Article 9, paragraph 1 (b)
Criterion 24	Article 9, paragraph 1 (b)
Criterion 25	Article 9, paragraph 1 (b)
Criterion 26	Article 10 (b)
Criterion 27	Article 9, paragraph 1 (b)

Table 6-1 Correspondence between the Developed Criteria and the UNCITRAL Law Articles

Table 6-1 shows that criterion 5 does not link to any of the UNCITRAL law articles, and criterion 5 requires that there should be a dispute referee or arbitrator if there is any dispute arising between a CA and a subject. This requirement integrates with the role and mission of the United Nations because one of the purposes of the United Nations is to play the role of arbitrator in solving international economic, social, cultural and humanitarian problems [108].

6.3 Conclusion

In this chapter, we have examined the criteria we developed to show, first, their extent in complying with requirements stated in international law and second, to measure their degree of effectiveness when comparing practices embedded in international law. As an example international law, we used the United Nations Commission on International Trade Law (UNCITRAL) which defines a legal framework for using electronic signatures. We conclude that the criteria have been defined adequately based on the fact that they handled all the relevant UNCITRAL law articles, and this implies that they have a basis in the law of international trade which can be considered as strong supportive evidence for the accuracy of the decisions made using the criteria when used for comparison. This also implies that the semantic analysis has led us to define adequate criteria for estimating a subject's trustworthiness.

CHAPTER 7

CASE STUDY

7.1 Introduction

In this chapter a case study is used to illustrate that the criteria adequately fulfill our requirements and cover a real CA's CP. We are sure that the criteria will survive this testing; this feeling comes from the realisation that the criteria were extracted from CPs adopted by organizations well recognized in their communities. In addition, these criteria have shown their compliance with the UNCITRAL law articles that regulate the use of digital signatures amongst the 192 members of the United Nations [109] which almost makes it an international law.

For the case study, we consider a scenario wherein Alice receives a certificate from Bob signed by the private key of GlobalSign CA. Alice does not know or trust Bob's certificate issuer; therefore, Alice uses the criteria to determine if Bob's certificate is trustworthy or not. The case study will illustrate the authentication process step by step by comparing the criteria with the GlobalSign CP. At the end of this process the level trustworthiness of the GlobalSign CP will be decided upon to assist in accepting or rejecting the subject's certificate. This chapter will help in explaining the techniques introduced in Chapter 5: the XML representation and the numerical evaluation system. First, we start with criteria formalisation.

7.2 Criteria Formalisation

In Chapter 5 we introduced the formalisation for each criterion, but in order to use them to perform the comparison process we need to unite them in single XML file. Appendix D shows the complete formalisation of the developed criteria.

Under the section "Applying the formalisation process" in Chapter 4, we mentioned that our target of using XML schema was to build a framework and the idea behind that is shown in figure 4-1. We have accomplished this aim and have built the schema

upon the developed criteria. For reasons of size (2035 lines), we have included the schema “criteria-schema.xsd” on the attached CD. The schema developed has the ability to handle the following functions:

- Validating the XML representation of the developed criteria or the subject CP.
- Easing the creation of the XML representation of the subject CP.
- Handling choices available for performing any of the acts.

For the purpose of the comparison process we need to add a new obligation title to the previous ones already defined in Chapter 4 which is “notDefined”. This new obligation title will be the value of the subject CP when the subject CP does not cover what has been requested in the corresponding criterion.

The result of applying the developed criteria to a real case is described in the following section.

7.3 GlobalSign Certification Authority CP

GlobalSign Certification Authority (hereinafter, GlobalSign CA) issues top level certificates, which are also known as root or anchor certificates (OmniRoot), to third party CAs that seek to enter GlobalSign’s certificate hierarchy. The GlobalSign CP can be found on its CA repository at <https://www.globalsign.net/repository>. The company is located in Belgium [110] .

7.4 Authenticating the GlobalSign CP

In this section we use the following steps to authenticate the GlobalSign CP based on the developed criteria:

1. First, we quote passages from the GlobalSign CP which deal with the issues that have been dealt with by corresponding criterion.
2. We discuss to what extent the quoted passages of the GlobalSign CP meet what is articulated in the corresponding criterion.
3. We show the XML representation of the quoted passages.
4. Finally, we state the weight for the quoted passages.

7.4.1 Compliance with Criterion 1

Passage:

Subscribers of GlobalSign Omniroot are third party CAs that seek to be issued with certificates within a hierarchy managed by GlobalSign. Subscribers of GlobalSign services are also natural or legal persons that successfully apply for a CA certificates.

Legal persons must be duly represented by an authorised agent (e.g. an authorised Director).

Subscribers legal persons which are natural persons, are conditionally accepted as subscribers for CA chaining services. The relationship of these persons with the CA to be chained to has to be duly explained and justification must be provided to GlobalSign.

Justification:

The quoted passages do not meet what has been stated in criterion 1 exactly, but there is indirect assurance which can be inferred from the above passages, thus:

1. The certified subject is a third party CA which means that it is reliable enough to manage CA tasks and has gained the required knowledge of adhering to the GlobalSign CP.
2. Constraints applied when non-authorised agents are to be certified.

Taking the implicit meaning of the quoted passages with the absence of explicit declaration of what should satisfy criterion 1, we classify the above as **<possible>**. The reason behind this is because the above justification could be satisfied by one subscriber but not by others.

XML representation:

```
<Criterion1>
  <CertificationAuthority>
    <possible>
      <checking>
        <capability of="subject" toManage="subordinate CA">
          <requirement>
            <withCompliance with="agreed CP"/>
          </requirement>
        </capability>
      </checking>
    </possible>
  </CertificationAuthority>
</Criterion1>
```

Weight:

According to table 5-1, we assign the following weights for the quoted passages:

Obligation Title	Action	Constraint	Total
0	1	1	2

7.4.2 Compliance with Criterion 2

Passage:

The definition section, Registration Authority reads:

*An entity that has the responsibility to identify and authenticate subscribers.
The RA does not issue certificates. It merely requests the issuance of a
certificate on behalf of applicants whose identity it has verified.*

Justification:

The quoted passage complies exactly with criterion 2.

XML representation:

```
<criterion2>
  <RegistrationAuthority>
    <prohibition>
      <issue>
        <certificates to="subject"/>
      </issue>
    </prohibition>
  </RegistrationAuthority>
</criterion2>
```

Weight: *GlobalSign maintains sufficient resources to meet its perceived obligations under this CP.*

According to table 5-1, the weight for the quoted passage:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.3 Compliance with Criterion 3

Passage:

GlobalSign maintains sufficient resources to meet its perceived obligations under this CP.

Justification:

The quoted passage complies exactly with criterion 3.

XML representation:

```
<critrion3>
  <participant>
    <requirement>
      <declare>
        <financialResponsibility for="its liabilities" to="other participants"/>
        <assets to="support its operations and liabilities"/>
      </declare>
    </requirement>
  </participant>
</critrion3>
```

Weight:

Due to the similarity, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
1	2	0	3

7.4.4 Compliance with Criterion 4

Passage:

This CP is governed, construed and interpreted in accordance with the laws of Belgium.

The laws of Belgium apply also to all GlobalSign commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to GlobalSign products and services where the GlobalSign acts as a provider, supplier, beneficiary receiver or otherwise.

Justification:

The quoted passages comply exactly with criterion 4.

XML representation:

```
<Criterion4>
  <CertificationAuthority>
    <requirement>
      <ensure>
        <law ofCountry="BE" governsAnyAgreement="true">
          <requirement>
            <sameCountry where="CA" isEstablished="true"/>
          </requirement>
        </law>
      </ensure>
    </requirement>
  </CertificationAuthority>
</Criterion4>
```

Weight:

The quoted passages weight is:

Obligation Title	Action	Constraint	Total
1	1	1	3

7.4.5 Compliance with Criterion 5

Passage:

If the dispute is not resolved within (20) days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with art. 167 6-1723 of the Belgian Judicial Code.

Justification:

Criterion 5 stated exactly the same things as in the quoted passage.

XML representation:

```
<Criterion5>
  <CertificationAuthority>
    <requirement>
      <allow>
        <arbitration to="resolve disputes arising out of its CP"/>
      </allow>
    </requirement>
  </CertificationAuthority>
</Criterion5>
```

Weight:

According to table 5-1, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.6 Compliance with Criteria 6

Passage:

To carry out the audits, there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with GlobalSign nor having any conflicting interests thereof.

Justification:

GlobalSign CP has covered criterion 6 which requires an external auditor as the quoted passage states.

XML representation:

```
<Criterion6>
  <CertificationAuthority>
    <requirement>
      <perform>
        <process of="compliance Audit">
          <requirement>
            <carryOut by="external auditor"/>
          </requirement>
        </process>
      </perform>
    </requirement>
  </CertificationAuthority>
</Criterion6>
```

Weight:

Due to adequacy, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
1	1	1	3

7.4.7 Compliance with Criteria 7

Passage:

GlobalSign does not provide further information about performing frequent audits.

Justification:

Frequency of audit (covered by criterion 7) has not been defined in the GlobalSign CP. Therefore the XML statement that defines the frequency includes the obligation title “notDefined”.

XML representation:

```
<Criterion7>
  <CertificationAuthority>
    <notDefined>
  </notDefined>
  </CertificationAuthority>
</Criterion7>
```

Weight:

Due to incomplete information, the weight is:

Obligation Title	Action	Constraint	Total
0	0	0	0

7.4.8 Compliance with Criterion 8

Passage:

The CA evaluates the results of such audits before further implementing them.

Justification:

The only action that is mentioned in the CP is the above passage, and this does not comply with requirement defined in criterion 8.

XML representation:

```
<Criterion8>
  <CertificationAuthority>
    <notDefined>
  </notDefined>
  </CertificationAuthority>
</Criterion8>
```

Weight:

Due to non-compliance, the weight is:

Obligation Title	Action	Constraint	Total
0	0	0	0

7.4.9 Compliance with Criterion 9

Passage:

GlobalSign does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the GlobalSign owes a duty to keep information confidential is the party requesting such information.*
- A court order.*

Justification:

GlobalSign complies with criterion 9.

XML representation:

```
<Criterion9>
  <CertificationAuthority>
    <prohibition>
      <discloseTo>
        <thirdParties any="confidential information" of="subject">
          <requirement>
            <except>
              <whenRequestedByLaw>true</whenRequestedByLaw>
              <whenConsentBySubject>true</whenConsentBySubject>
            </except>
          </requirement>
        </thirdParties>
      </discloseTo>
    </prohibition>
  </CertificationAuthority>
</Criterion9>
```

Weight:

The quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	2	4

7.4.10 Compliance with Criterion 10

Passage:

GlobalSign accepts other CAs wishing to enter its own network and operate under its own hierarchy. Following an initial assessment and the signing of a specific agreement with GlobalSign the applicant CA has to provide GlobalSign with certain identification documents including an authorisation letter, articles of association. GlobalSign retains its right to consult third party databases that identify organisations in this regard.

GlobalSign or an authorized GlobalSign RA verifies by appropriate means and on the basis of a document procedure, the identity and, if applicable, all attributes thereof of applicants of a certificate. In addition to the above, to identify organizations GlobalSign typically request certified copies of by-laws, and possibly additional identification elements such as proof of VAT registration etc.

Justification:

The criterion requests that organization identity authentication should include information about the organization's publicity and popularity, and the quoted passages satisfy this with the following clauses:

- *CA has to provide GlobalSign with certain identification documents including an authorisation letter, articles of association*
- *GlobalSign retains its right to consult third party databases that identify organisations in this regard.*
- *GlobalSign typically request certified copies of by-laws, and possibly additional identification elements such as proof of VAT registration etc.*

XML representation:

```
<Criterion10>
  <RegistrationAuthority>
    <requirement>
      <authenticate>
        <organization include="its reputation"/>
      </authenticate>
    </requirement>
  </RegistrationAuthority>
</Criterion10>
```

Weight:

The quoted passages weight is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.11 Compliance with Criterion 11

Passage:

CA chaining services do not require the physical appearance of the customer as long as an agreement between the applicant organization and GlobalSign has been executed.

Justification:

GlobalSign restricts certificate issue to subscribers, third party CAs, or to subjects associated with a subscriber which called a “Certificate Applicant”; as stated in [110] that certificate applicant can be any person acting on behalf of the subject. Therefore; the quoted passage states clearly that because of the agreement between the applicant organization and GlobalSign physical appearance is not required. We assume that a certificate applicant will do the authentication by physical appearance, and also we assume that this requirement could be omitted, and this case is covered under the “possible” obligation title.

XML representation:

```
<Criterion11>
  <RegistrationAuthority>
    <possible>
      <authenticate>
        <individual basedOn="its physical presence"/>
      </authenticate>
    </possible>
  </RegistrationAuthority>
</Criterion11>
```

Weight:

Due to the assumption we made which is that it might or might not happen, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
0	1	0	1

7.4.12 Compliance with Criterion 12

Passage:

Before entering any contractual relationship with the subscriber, GlobalSign makes available a CA chaining agreement, which the applicant must approve prior to placing a request with GlobalSign.

Justification:

The quoted passage complies with criterion 12.

XML representation:

```
<Criterion12>
  <CertificationAuthority>
    <requirement>
      <insure>
        <subject isAwareOf="its respective rights and obligations"/>
      </insure>
    </requirement>
  </CertificationAuthority>
</Criterion12>
```

Weight:

The quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.13 Compliance with Criterion 13

Passage:

Under section “CRL Profile”, the table that shows the profile of the GlobalSign Revocation List states in “Next Update” cell the following:

[Date of issuance + 3 hours]

Justification:

Criterion 13 requests the update of CRL must take place within an hour and the quoted passage says after three hours.

XML representation:

```
<Criterion13>
  <CertificationAuthority>
    <requirement>
      <update>
        <CRL after="every certificate revocation">
          <requirement>
            <updateIntervalTime withIn="3"/>
          </requirement>
        </CRL>
      </update>
    </requirement>
  </CertificationAuthority>
</Criterion13>
```

Weight:

Criterion 13 reduces the interval time of updating CRL to one hour which is more effective in blocking any specious behaviour after the compromise of a certificate. Therefore; the quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.14 Compliance with Criterion 14

Passage:

The interval time to update the CRL in the GlobalSign is 3 hours which is also the validity period of the CRL.

[Date of issuance + 3 hours]

Justification:

Criterion 14 defines the validity period of the CRL as 30 days which is considered longer than 3 hours.

XML representation:

```
<Criterion14>
  <CertificationAuthority>
    <requirement>
      <publish>
        <CRL>
          <requirement>
            <intervalTime withIn="3 hours"/>
          </requirement>
        </CRL>
      </publish>
    </requirement>
  </CertificationAuthority>
</Criterion14>
```

Weigh:

The short validity period of the CRL may cause high traffic but it provides relying parties with almost real-time certificate-status information; therefore, the quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	1	3

7.4.15 Compliance with Criterion 15

Passage:

GlobalSign CA audit records events that include but are not limited to

- Issuance of a certificate
- Revocation of a certificate
- Published CRLs

Justification:

The quoted passage covers some of the records defined by criterion 15.

XML representation:

```
<Criterion15>
  <CertificationAuthority>
    <requirement>
      <do>
        <securirtyAudit>
          <requirement>
            <allBootsOfThePKISystem>>false</allBootsOfThePKISystem>
            <allAccessAttemptsToPKISystem>>false</allAccessAttemptsToPKISystem>
            <allPKISystemFailures>>false</allPKISystemFailures>
            <CAkeyGeneration>>false</CAkeyGeneration>
            <CAkeyStorage>>false</CAkeyStorage>
            <CAkeyBackup>>false</CAkeyBackup>
            <CAkeyArchival>>false</CAkeyArchival>
            <CAkeyRecovery>>false</CAkeyRecovery>
            <CAkeyDestruction>>false</CAkeyDestruction>
            <CAandSubjectCertificate>
              <generationRequests>>false</generationRequests>
              <renewalRequests>>false</renewalRequests>
              <re-keyRequests>>false</re-keyRequests>
              <revocationRequests>>true</revocationRequests>
            </CAandSubjectCertificate>
            <issuanceOfCertificates>>true</issuanceOfCertificates>
            <certificateRequests>
              <ofStatusChange>>false</ofStatusChange>
              <ofStatus>>false</ofStatus>
              <responses>>false</responses>
            </certificateRequests>
            <PKIandSecuritySystemActions>
              <performedByCApersonnel>>false</performedByCApersonnel>
            </PKIandSecuritySystemActions>
            <identityVerificationProcedures>>false</identityVerificationProcedures>
          </requirement>
        </securirtyAudit>
      </do>
    </requirement>
  </CertificationAuthority>
</Criterion15>
```


Weight:

The quoted passage omits a number of events that are not included in the ones shown on above list, thus the weight is:

Obligation Title	Action	Constraint	Total
1	1	2	4

7.4.16 Compliance with Criterion 16

Passage:

GlobalSign CA ensures that designated personnel reviews log files at regular intervals detects and reports anomalous events.

Justification:

The quoted passage states that log files are reviewed at regular intervals but there is no defined interval we could compare to the value defined in criterion 16.

XML representation:

```
<Criterion16>
  <CertificationAuthority>
    <requirement>
      <examine>
        <auditLogs>
          <requirement>
            <frequent atLeast="notDefined"/>
          </requirement>
        </auditLogs>
      </examine>
    </requirement>
  </CertificationAuthority>
</Criterion16>
```

Weight:

According to the table 5-1, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.17 Compliance with Criterion 17

Passage:

GlobalSign CP does not cover this requirement.

Justification:

The requirement requested by criterion 17 is not covered by the GlobalSign CP.

XML representation:

```
<Criterion17>
  <CertificationAuthority>
    <notDefined>
  </notDefined>
  </CertificationAuthority>
</Criterion17>
```

Weight:

The GlobalSign weight with respect to this requirement is:

Obligation Title	Action	Constraint	Total
0	0	0	0

7.4.18 Compliance with Criterion 18

Passage:

GlobalSign CA retains in a trustworthy manner records of GlobalSign CA digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

GlobalSign CA keeps internal records of the following items:

- CA certificates for a period of a maximum of 10 years after the expiration of the certificate.*
- Audit trails on the issuance of CA certificates for a period of 5 years after issuance of a certificate.*

- *Audit trail of the revocation of a CA certificates for a period of 5 years after revocation of a certificate.*
- *CRLs for a minimum of 5 years after expiration or revocation of a CA certificate.*
- *Support documents on the issuance of CA certificates for a period of 5 years after expiration of a certificate.*

Justification:

The quoted passages only meet a subset of the criterion 18 requests that records should be archived, but it complies with the retention period.

XML representation:

```
<Criterion18>
  <CertificationAuthority>
    <requirement>
      <provide>
        <archiving>
          <requirement>
            <certificateRequestApplication>true</certificateRequestApplication>
            <documentationSupportingCertificateApplications>true</documentationSupportingCertificateApplications>
            <allComputerSecurityAuditData>true</allComputerSecurityAuditData>
            <certificateRevocationApplication>true</certificateRevocationApplication>
            <certificateRe-keyApplication>false</certificateRe-keyApplication>
            <certificateRenewalApplication>false</certificateRenewalApplication>
            <issuedCertificates>true</issuedCertificates>
            <issuedCRLsORcertificateStatusRecords>true</issuedCRLsORcertificateStatusRecords>
            <allcorrespondence>
              <betweenTheCAandSubcontractors>false</betweenTheCAandSubcontractors>
              <betweenTheCAandSubscribers>false</betweenTheCAandSubscribers>
            </allcorrespondence>
            <retentionPeriod>
              <atLeast InYears="5"/>
            </retentionPeriod>
          </requirement>
        </archiving>
      </provide>
    </requirement>
  </CertificationAuthority>
</Criterion18>
```

Weight:

Due to the lack of archived records, the quoted passages weight is:

Obligation Title	Action	Constraint	Total
1	1	7	9

7.4.19 Compliance with Criterion 19

Passage:

GlobalSign CA documents the recovery procedures used if computing resources, software, and/or data corrupted or suspected of being corrupted.

Justification:

The quoted passage complies exactly with criterion 19.

XML representation:

```
<Criterion19>
  <CertificationAuthority>
    <requirement>
      <establish>
        <plan of="surviving after the disaster"/>
      </establish>
    </requirement>
  </CertificationAuthority>
</Criterion19>
```

Weight:

The weight which is assigned for the quoted passage according to table 5-1 is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.20 Compliance with Criterion 20

Passage:

GlobalSign CA reaches its subscribers through a designated Registration Authorities. An RA requests the issuance, suspension and revocation of a certificate under this CP.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

Justification:

All the trusted roles requested by criterion 20 are supported by the GlobalSign CP except the “System Operators” role.

XML representation:

```
<Criterion20>
  <CertificationAuthority>
    <requirement>
      <support>
        <trustedRoles>
          <requirement>
            <securityOfficers>true</securityOfficers>
            <registrationOfficers>true</registrationOfficers>
            <syemAdministrators>true</syemAdministrators>
            <systemOperators>false</systemOperators>
            <systemAuditors>true</systemAuditors>
          </requirement>
        </trustedRoles>
      </support>
    </requirement>
  </CertificationAuthority>
</Criterion20>
```

Weight:

Because the quoted passages has not fully met criterion 20, its weight is:

Obligation Title	Action	Constraint	Total
1	1	4	6

7.4.21 Compliance with Criterion 21

Passage:

The GlobalSign CA carries out checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Background checks include:

- *Misrepresentations by the candidate.*
- *Any other as it might be deemed necessary.*

The GlobalSign CA makes available training fro their personnel to carry out CA and RA functions.

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

GlobalSign CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

The GlobalSign CA, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.

Justification:

The quoted passages comply exactly with criterion 21.

XML representation:

```
<Criterion21>
<CertificationAuthority>
  <requirement>
    <assure>
      <allPersonnelControlled>
        <requirement>
          <backgroundChecked>
            <qualifications>true</qualifications>
            <experience>true</experience>
            <governmentClearances>true</governmentClearances>
          </backgroundChecked>
          <providingWthTaining>true</providingWthTaining>
          <povidingWthRefresherTaining>true</povidingWthRefresherTaining>
          <sanctioningForUnauthorizedActions>true</sanctioningForUnauthorizedActions>
          <providingWithDocumentation>true</providingWithDocumentation>
        </requirement>
      </allPersonnelControlled>
    </assure>
  </requirement>
</CertificationAuthority>
</Criterion21>
```

Weight: *Generating securely their private-public key pair, using a trustworthy*

Weight for the quoted passages is:

Obligation Title	Action	Constraint	Total
1	1	7	9

7.4.22 Compliance with Criterion 22

Passage:

Under section “Subscriber Obligations” the following is stated:

Generating securely their private-public key pair, using a trustworthy system.

Justification:

The quoted passage meets with what has been stated in criterion 22.

XML representation:

```
<Criterion22>
  <subject>
    <requirement>
      <generate>
        <itsKeys>true</itsKeys>
      </generate>
    </requirement>
  </subject>
</Criterion22>
```

Weight:

Due to compliance with criterion 22, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.23 Compliance with Criterion 23

Passage:

For the CA Root key it uses, the GlobalSign CA makes use of the RSA algorithm with a key length of either 1024 or 2048 bits and validity period of at least 14 years.

For the operational CA keys it uses the GlobalSign CA makes use of the RSA algorithm with a key length of 1024 bits and a validity period of up to 7 years.

Justification:

The key length included in the quoted passages is consistent with the one defined in criterion 23.

XML representation:

```
<Criterion23>
  <CertificationAuthority>
    <requirement>
      <makeSure>
        <minimumLength of="private key" isInBits="1024"/>
      </makeSure>
    </requirement>
  </CertificationAuthority>
</Criterion23>
```

Weight:

The quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.24 Compliance with Criterion 24

Passage:

The passage quoted above stated that the validity period of a CA Root key is at least 14 years and the validity period of operational CA keys is up to 7 years.

Justification:

GlobalSign CA issues top root certificates and criterion 24 limits the validity period for CA certificate to be up to 20 years. Thus, what has been stated in the quoted passage complies with criterion 24. The second part of criterion 24 is not applicable here because it defines a key validity period for non root certificate.

XML representation:

```
<Criterion24>
  <CertificationAuthority>
    <prohibition>
      <create>
        <CAcertificateValidityPeriods moreThanInYears="20"/>
        <subjectCertificateValidityPeriods moreThanInYear="0"/>
      </create>
    </prohibition>
  </CertificationAuthority>
</Criterion24>
```

Weight:

Due to compliance with criterion 24 of CA certificate's validity period, the weight for the quoted passage is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.25 Compliance with Criterion 25

Passage:

The GlobalSign CA implements computer security controls.

Justification:

No further clarification which could assist us to judge the compliance with criterion 25 of these security controls occurs in the GlobalSign CP, so will mark it accordingly

XML representation:

```
<Criterion25>
  <CertificationAuthority>
    <requirement>
      <secure>
        <CAmachine>
          <requirement>
            <disconnectFromNetwork>false</disconnectFromNetwork>
            <prohibitUnauthorizedAccess>false</prohibitUnauthorizedAccess>
            <updatingOSwithSecurityPatches>false</updatingOSwithSecurityPatches>
            <limitAccess>false</limitAccess>
          </requirement>
        </CAmachine>
      </secure>
    </requirement>
  </CertificationAuthority>
</Criterion25>
```

Weight:

The lack of clarity of what security controls are implemented leads us to conclude that the quoted passage is not adequately defined; therefore; its weight is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.26 Compliance with Criterion 26

Passage:

The GlobalSign CA performs periodic development controls and security management controls.

Justification:

The controls stated in the quoted passage are not listed in detail in the GlobalSign CP which does not allow us to check for compliance with criterion 26. For this reason, we

weight the obligation title and the action parts but the constraints are set to the value false.

XML representation:

```
<Criterion26>
  <CertificationAuthority>
    <requirement>
      <examining>
        <integrityOfHardwareAndSoftwareBy>
          <requirement>
            <documentedAndControlledAny>
              <configuration>>false</configuration>
              <modifications>>false</modifications>
              <upgrades>>false</upgrades>
            </documentedAndControlledAny>
            <detectingUnauthorizedModification>>false</detectingUnauthorizedModification>
            <checkingSoftwareIntegrity>
              <atLeast inDays="0"/>
            </checkingSoftwareIntegrity>
          </requirement>
        </integrityOfHardwareAndSoftwareBy>
      </examining>
    </requirement>
  </CertificationAuthority>
</Criterion26>
```

Weight:

The quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	0	2

7.4.27 Compliance with Criterion 27

Passage:

The GlobalSign CA maintains a high-level network of systems security including firewalls. Network intrusions are detected. In specific:

- The GlobalSign CA encrypts connections to the RA, using dedicated administrative certificates.*

- *The GlobalSign CA website provides certificate based Secure Socket Layer connections and anti-virus protection.*
- *The GlobalSign CA network is protect by a managed firewall and intrusion detection system.*
- *Internet sessions for request and delivery of information are encrypted.*

Justification:

The quoted passage complees exactly with criterion 27.

XML representation:

```

<Criterion27>
  <CertificationAuthority>
    <requirement>
      <securing>
        <networks>
          <requirement>
            <firewalls>true</firewalls>
            <encryptionAndDigitalSignatures>true</encryptionAndDigitalSignatures>
            <ACLs>true</ACLs>
          </requirement>
        </networks>
      </securing>
    </requirement>
  </CertificationAuthority>
</Criterion27>

```

Weight:

All the actions defined by criterion 27 needed to be taken to secure the network are implemented in the GlobalSign CP; therefore; the quoted passage weight is:

Obligation Title	Action	Constraint	Total
1	1	3	5

7.5 Authentication Result

We have assigned all the correspondences to criteria in the GlobalSign CP their values and can use equation (1) to calculate the ND value. After applying equation (1), the ND value for GlobalSign CP is 76. The GlobalSign CP complies with the

developed criteria at more than 63%. The ND value classifies the relation between the developed criteria and the GlobalSign CP as a partial overlap. According to the scenario given at the start of this chapter, Alice does not know GlobalSign; therefore, the partial overlap between the criteria and GlobalSign CP is not acceptable. With this attribute the answer to Alice is that GlobalSign is not a trusted CA. The result of the comparison is not an abnormal result, because GlobalSign CP deals with top level CAs and for this reason most of the issues targeting non-CA subjects are omitted. This is because either some of the issues are not applicable in the case that the subjects are CAs, or because these issues are already known to these types of subjects and do not need to be mentioned in the CP.

Let us consider another scenario where Alice has received a certificate that has been signed by VeriSign Inc. We selected this scenario as VeriSign issues certificates to end entities as well to CAs; therefore, the VeriSign CP must deal with related issues more comprehensively than GlobalSign’s CP. The authentication of VeriSign’s CP [55] is summarized in table 7-1 (the complete process is as explained for the previous scenario).

Criterion	Weighting			Criterion	Weighting			Criterion	Weighting		
	Obligation Title	Action	Constraint		Obligation Title	Action	Constraint		Obligation Title	Action	Constraint
1	1	1	1	10	1	1	NA	19	1	1	NA
2	1	1	NA	11	0	1	NA	20	1	1	4
3	1	2	NA	12	1	1	NA	21	1	1	7
4	1	1	1	13	1	1	0	22	1	1	NA
5	1	1	NA	14	1	1	1	23	1	1	NA
6	1	1	1	15	1	1	11	24	1	1	NA
7	1	1	1	16	1	1	0	25	1	1	3

8	1	1	1	17	1	1	NA	26	1	1	6
9	1	1	2	18	1	1	11	27	1	1	3

Table 7-1 VeriSign CP Authentication

The ND value for VeriSign CP is 107: partial overlap; thus the compatibility of the VeriSign CP with the criteria is 89%. The ND value of the VeriSign CP is obviously better than that of GlobalSign CP; however, the answer to Alice is that VeriSign is also not a trusted CA.

7.5.1 Result Discussion

Despite the selected CAs, GlobalSign and VeriSign, being well-known and considered to be leading organizations in offering PKI services, the two scenarios show their failure to satisfy the criteria authentication process. These results appear to contradict with the organizations' reality but we should recall that the criteria are designed to be worked in the absence of trusted domain and they assist in evaluating the level of trust that can be placed on a subject's certificate by examining the CP that operates its certificate. This fact necessitates careful evaluation of the subject CP by requiring it to have specific values which are considered optimal for untrusted domains. We conclude by noting that the evaluated organizations are well-known CAs but because their values under certain issues do not match the criteria, the result in the two scenarios is partial overlap. Ultimately, there is no perfect scoring system and we have included in the future work section, chapter 8, the issue of improving the scoring system.

7.6 Conclusion

The purpose of this chapter was to show the applicability of the criteria developed to a real CP. The GlobalSign CA, a leader in public trust services, has been issuing public certificates since 1996. We selected GlobalSign to show how the criteria coped with its CP. The reason behind selecting GlobalSign was that, as a leading company, we are sure that it will maintain its services robustly and this should lead to the writing of a robust CP. Therefore, applying the developed criteria on this CP will give a clear

view of their applicability and the coverage in their results. We then examined the applicability of the criteria to the VeriSign CP due to the GlobalSign CP not addressing some policy issues. These case studies showed that the criteria handled the correspondence activities defined in GlobalSign and VeriSign CPs sufficiently well.

CHAPTER 8

CONCLUSIONS AND FUTURE WORK

8.1 Discussion

The main goal of this dissertation was to find a way to authenticate a subject certificate in an untrusted domain. The first question that we investigated was how to authenticate a certificate in a domain that we do not know much about. As we have to authenticate a certificate that has been issued by an unknown CA, we are forced to judge the procedures, controls, obligations, liabilities and indemnities used by the CA, all of which are stated in the CA's CP. Therefore, investigating the CA's CP is offered as a way of producing a decision about a CA's trustworthiness. In order to use the CP for authenticating a subject certificate we used a formalisation technique.

Chapter 4 began by applying our approach to comparing the CPs of an untrusted CA and an already trusted CA, and it presented a description of the processes used to develop a formalisation technique. The ultimate goal of chapter 4 was to build a semantic representation of a CP.

The process was started by selecting the EuroPKI CP with the aim of capturing its semantics using XML to build the formalisation. We realized that it was necessary to produce identical representations of identical items that were expressed differently, so we defined a number of conventions that the process used in order to achieve this. After finishing the formalisation and examining the outcomes: 40 XML files and 37 schema files, we concluded that we could not achieve our target. The reason for this being that the formalisation process was based on the exact interpretation of what had been written in the EuroPKI CP. We decided to change our approach in order to improve the way the formalisation was created, based on first finding out how we could represent the semantics in the formalisation.

The second stage of the formalisation focused first on finding a way to incorporate semantics into the CP formalisation. Throughout the first stage of the formalisation,

which was accomplished by formalising the whole of the EuroPKI CP, we found that there were certain words expressing the level of importance of the task described in the CP. After we studied these words again, we realized that a CP is nothing but a set of rules that regulate certificates and their applicability; therefore; these words do indeed describe the semantics of the rules. The formalisation for this stage was carried out through using these words after grouping all words that depict the same level of importance together under varying titles (*requirement*, *prohibition*, *preferred*, *not preferred* and *possible*). The policies we used in this stage were EuroPKI, DutchGrid, State of Illinois, SwuPKI and VeriSign. Because there were 5 CPs, we decided to formalise only the section “Community and applicability”, so we can get this stage’s outcomes as quickly as possible. We evaluated the outcomes of the five formalisations and found that these are almost the same which did not really help us in achieving an efficient comparison technique for measuring the level of a subject's trustworthiness.

From these stages of formalisation and analysis, we learned that to perform a comparison based on semantics, we needed to develop specific criteria that have the same names in the formalisation but that can differ in their values.

In the third stage, we knew our ultimate goal, and three CPs were selected for use: EuroPKI, SwuPKI and DutchGrid. The formalisation process was initiated differently from the two previous stages, and we started by comparing the textual content of the CPs manually after entering them in a table with three columns covering 106 pages. This time the comparison was performed by comparing each section separately in the participating CPs. The method that we use to select the criteria was:

1. Find the criteria that have been emphasised in participating CPs.
2. Find the criteria that themselves playing significant roles in defining obligations.

After finishing this manual comparison, we identified 43 criteria. As these criteria were a result of a manual comparison process, they need to be studied and analysed to satisfy the following conditions:

1. Filter out unrelated criteria.

2. Represent crucial information required for the comparison process.

For the above conditions we chose Annex II of The European Directive [Dir.1999/93/EC] [28] which is a regulation for certification service providers when issuing qualified certificates. The results of this are summarized in the following:

1. The number of the criteria decreased to 22.
2. There are requirements in the Directive that do not match any criteria.
3. The Directive covers certification service providers who are known to relying parties. We need to define more requirements to cover the case of unknown certification service providers.

Considering point 3, we finally defined 27 criteria to be used when performing authentication of a subject's identity by comparing our criteria to what has been written in the relevant CA's CP.

Chapter 5 finishes the work started in the previous chapter. We mentioned "semantics" often in previous chapters and said that the formalisation would be based on them. In this chapter, we began by defining this concept for each criterion and showed how it is related to the subject's trustworthiness. The overall objective for all criteria is to provide an extra level of assurance about the subject's certificate in addition to the assurance that is provided by the issuer CA.

All the 27 defined criteria are in textual form and, as we said earlier, XML was to be used for formalisation. However, the formalisation by itself is not capable of producing an efficient comparison approach; we need first to specify a defined value for each criterion to assist us in doing the comparison. Therefore, we met this requirement for each criterion, and afterwards the formalisation of each criterion with its defined value was also done using XML.

Performing a comparison between the criteria and a subject's CP will result in a number of similarities between them and a number of differences. Accordingly, it was necessary to find a way to represent the result in a more formal way: we developed a scoring system to assign a weight to each criterion according to the result of the comparison that is defined in the system. Furthermore, we developed an equation to

produce a numeric decision value (ND) as a result of comparing the developed criteria to the subject's CP.

Finally, we studied in detail the ND value which allows us to make a more precise interpretation based on it. The ND value for our criteria is 120 and by comparing the ND value of the subject's CP, we observe three cases depicting the trustworthiness of the subject. The first case is when there is no trust we could place on the subject's certificate and we called this case "no overlap"; this happens when the subject ND value is 0. The second case is when the subject ND value is between 0 and 120, and means that we can trust the subject for certain activities but not all. We call this case "partial overlap". The third case occurs when the subject ND value is exactly 120 which shows that the subject's trustworthiness is equal to that of the developed criteria. We called this case "absolute overlap".

Chapter 6 was mainly an examination of the criteria developed and the examination then focused on clarifying the following issues:

1. The extent that the developed criteria comply with requirements in international law.
2. Degree of their effectiveness compared with practices embedded in international law.

We used the United Nations Commission on International Trade Law (UNCITRAL) [102] which defines a legal framework for using electronic signatures as a test for the examination process for the criteria. The result of this showed that the criteria are handled totally by UNCITRAL law articles, and this implies that they have been adequately defined. Moreover, the examination process shows that the semantic analysis has led us to define adequate criteria for estimating a subject's trustworthiness.

Finally, after we demonstrated the robustness and coverage of the developed in the previous chapter, we were obliged to prove this claim by implementing the criteria on a real life case. GlobalSign CA was selected for implementation of the criteria on its CP. In order to accomplish this task, we followed the following scenario:

1. We quote a passage from the GlobalSign CP which deals with the same task that the selected criterion deals with.
2. We discuss the suitability and incompatibility with the selected criterion.
3. We format the XML representation for the quoted passage.
4. We specify the weight for the quoted passage depending on what has stated in point 2.

The above process continued until all the criteria had been processed; afterwards, we applied the equation (1). The GlobalSign ND value is 76 which describes the relationship between its CP and the developed criteria as a partial overlap. We followed this case study with another one which examines the applicability of the criteria against the VeriSign CP. For a more detailed explanation about the case studies see Chapter 7. We conclude that the developed criteria adapted to the real life cases without any deficiencies or shortages in coverage. The implication of this is that the criteria can be applied in reality and do measure the trustworthiness of the subject efficiently.

In summary, the work that has been done in this thesis is a contribution to help in leveraging PKI technology on the Internet. We stated clearly in the beginning chapters of this thesis that integrating PKI technology with the Internet required the presence of a third party (a trusted CA) which vouches for the identity of the subject and this vouching is accepted by relying parties because they trust the issuer of the certificate. We raised the point that if the trusted CA or trust anchor is not available, then we have an untrusted domain. What if there is a service that we would like to have but which has a certificate issued by an unknown CA? Do we reject the service for this reason or can we develop a technique that can help in authenticating the subject's certificate even if it is in an untrusted domain? Authenticating or validating certificate in PKI technology is based on the construction of a certification path connecting the subject's certificate with the relying party's trusted anchor. In an untrusted domain with no presence of a trusted anchor, the process of building the certification path is considered unreasonable. However, with our criteria, a direct certification path can be constructed by applying the criteria's results for the subject's certificate CP and the result being "absolute overlap". The direct certification path results from the fact that the authenticating process involves applying the criteria

showing the validation of the subject certificate's CP as meeting the requirements that they set.

In the case of a trusted domain where a relying party has a trusted point, the scenario is different where there is a certification path that leads to the trusted point. The role of the criteria in this case changes from validating only the subject certificate to different role as illustrated in next. Let us emphasize that the criteria can work and be applied in the case of trusted domain as they were developed based on the certificate policy framework which is considered as a guideline for developing CP. Moreover, they are extracted from real, operational CPs. If the criteria are applied to an issuer that is trusted by the relying party, the result will boost the relying party's confidence if it is "absolute overlap" and, in the terminology of certification paths, criteria with the result of "absolute overlap" assure that the constructed certification path is the best path by validating the CP or CPs that provide all the certificates on the constructed path. This is almost equivalent to the process of constructing a path between the criteria and the trusted issuer CP. If the result is "no overlap" or "partial overlap", the result could be rejected by the relying party because the criteria represent the optimal values and they include issues that are not of interest to the relying party. But in the case that the relying party accepts the "no overlap" or "partial overlap" result, this could help the relying party find another certification path to the subject certificate that satisfies the criteria or by finding another trusted issuer whose CP meets the requirements laid down by the criteria.

Cross-certification is a special case of certificate issuance where the subject of the certificate is a CA. In cross-certification, each CA agrees to accept each other's CPs. Therefore, the relying party in one domain trusts certificates in other domain. In this case there is a path between the root CAs connecting the two domains and any certification path constructed from one domain includes this path to complete the certification path to the other domain. Here the criteria can play the following roles:

- The root CA could use the criteria to judge the certification path from another domain, and in the case of "absolute overlap", as we stated above, the confidence level is increased. On the contrary, if the result is one of the other cases then the root CA has the option of finding another trusted point to do

cross-certification or to ask other root CA to adopt changes in its CP to meet the criteria.

- The issuer CA of either domain could use the criteria as a measurement for the path that is initiated from the other end toward any subject in that domain. And upon the result of applying the criteria on all the CP or CPs covering the certificates included in the certification path to the subject's certificate, the root CA's confidence about the constructed certificate path could be increased or it can look for other path that satisfies the criteria's requirements for use as a qualified path.

In a Bridge CA environment, the criteria could be used to guide the relying party to compare different CAs participating in the Bridge CA to base its decision to join or get services from a candidate CA. The relying party will be more likely to choose the CA whose criteria result is "absolute" rather than "partial" or "no overlap" results.

8.2 Future Work

This dissertation describes how to authenticate an X.509 certificate in an untrusted domain. There are several directions in which this work can be extended. We list the most important of them here and extend them with a few additional issues.

8.2.1 Representing CPs Context More Systematically

Even though CPs are structured according to RFC 2527 (and also with RFC 3647), their specification supersedes that given in RFC 2527, which is considered as a framework for building certificate CP, however current CPs are not fully helpful or efficient when someone wants to extract data manually for the following reason:

- CPs are expressed in natural language and thus are more fully descriptive.
- Data related to specific tasks are scattered over the CP document.
- There are spelling mistakes, which result in meaning changing; for example the following text is found in EuroPKI CP [48]:

CA. A relying party MUST check CRLs when validating the use of a certificate. Moreover a relying party MUST ONLY use the certificate

for the proscribed applications and MUST NOT use the certificates for forbidden applications.

Here we see the word “prescribed” replaced with “proscribed” , changing the meaning totally and introducing a contradiction between two specifications.

- CPs are all copied from each other with only the titles changed to identify organizations: as a small experiment do a search in Google with the mistake that we mentioned in the previous point and see the result.
- CP sections contain repeated information which makes CP seem to be long.

Because of this, rewriting CPs in a new structure is considered as a research topic and we expect the result to be able to handle the following:

- Representing the CP in a more formal way.
- The new representation could facilitate embedding the CP in the certificate.
- Easy the process of extracting the criteria values.
- Avoid ambiguity and repetition.

8.2.2 Automating the Comparison

Due to the reasons explained in the previous section, automating the comparison process would demand the introduction of different techniques. A CP is written in natural language which leads there to be different written CPs that have the same meaning. They are written using synonymous words (e.g. “issue”, “create”). To facilitate automated comparison requires either defining all the words used in CPs after identifying all of them, or else using Artificial Intelligence (AI) to build a system to identified these words gradually (i.e. build an expert system [111].) Implementing automated comparison will be more practical and effective if the representation of the CP context is created more systemically. Building the automated comparison will ease the embedding it in web browsers as a plug-in. Moreover, it helps in creating more services such as systems that score CAs’ CPs and posts the results. By doing this we

could provide a service that is known as OCSP for evaluating CPs instead certificates. Investigating this topic will open the door for new authentication techniques.

8.2.3 The Criteria Developed

In this thesis we have applied our criteria to one real world case study, GlobalSign CP [110]. With more time and different real world case studies, we would like to extend the implementation phase. Moreover, we would like to study the possibility of integrating the criteria with other models which have the same interest so as to provide a more comprehensive authentication management technique.

8.2.4 Scoring System

We have developed a simple scoring system; we would like to study the possibility of developing the scoring system in such a way that defines core criteria that play a main role in the value of ND. In the sense that if any of these core criteria are missing this implies that the subject's certificate will not be qualified to be trusted.

8.2.5 Acceptance of Our Contribution

Most of thesis's chapters have been published in refereed conference proceedings which provide a some academic accreditation: see publications section. Next we intend to seek industry acceptance for our solution. The most active working group is the PKIX of the IETF which develops Internet standards needed to support an X.509-based PKI. The purpose of this is to have our contribution to be published as an IETF standard and this will contribute to our solution through getting valuable comments that will improve our contribution before it is accepted as a standard.

8.3 Closing Remarks

The problem of authenticating another party's identity on the Internet is a real one. In this thesis we have shown how to authenticate the identity of the subject even in the absence of a trust anchor. Today solutions are based on establishing a community of

trust where there is only one root CA which leads to segregation between the users. Indeed, it will lead to creating an environment where collaboration is difficult. Further research in this area is therefore vital.

REFERENCE

1. Man Young Rhee. *Internet Security: Cryptographic Principles, Algorithms, and Protocols*. 2003 [cited; 426].
2. Merriam-Webster Online Dictionary. [cited; Available from: <http://www.m-w.com>].
3. Dieter Gollmann, *Computer Security*. Second ed. 2006: John Wiley & Sons Ltd. 374.
4. Robert Bagwill, et al. *Security in Open Systems*. [cited].
5. Pinkerton Inc. *TOP SECURITY THREATS and MANAGEMENT ISSUES FACING CORPORATE AMERICA*. [pdf file] 2003 [cited].
6. SunGard Availability Services and Harris Interactive. *Harris Interactive Survey of Fortune 1000 Companies Reveals Serious Deficiencies in Disaster Preparation*. [Web page] 2004 [cited; Available from: http://www.sungard.com/journalists/global/harris_interactive_survey_of_fortune_1000_companies_reveals_serious_deficiencies_in_disaster_prepara.htm]
- also \paper\survey\Harris Interactive Survey of Fortune 1000 Companies Reveals Serious Deficiencies in Disaster Preparation.htm.
7. PricewaterhouseCoopers. *Information Security Breaches Survey 2006*,. 2006 [cited].
8. Giampaolo Bella, Stefano Bistarelli, and Simon N. Foley. *Soft Constraints for Security*,. 2004 [cited].
9. Thawte Inc, *The value of authentication*.
10. Free On-line Dictionary of Computing. [www] [cited 2003 6/10]; Available from: <http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Formal+Description+Technique>.
11. Shahrzade Mazaher and P. Roe. *A survey of state of the art in Public Key Infrastructure*. [pdf file] 2003 [cited].
12. Karttaavi, T. and S.V. Rajan. *Identification of ISOC members: PKI requirements*. 2004 [cited; Available from: <http://www.isoc.fi/isoc-pki/whitepaper.html>].
13. Rick LaRowe. *Public Key Infrastructure (PKI) and Its Application in the New Economy*. 2000 [cited].
14. A. Arsenaault and S. Turner. *Internet X.509 Public Key Infrastructure: Roadmap*. 2002 July [cited; 57].
15. INTERNATIONAL TELECOMMUNICATION UNION, *RECOMMENDATION X.509, ISO/IEC 9594-8: INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - THE DIRECTORY PUBLIC-KEY AND ATTRIBUTE CERTIFICATE FRAMEWORKS*. 2001: p. 162.
16. C. Enrique Ortiz (2005) *The Security and Trust Services API (SATSA) for J2ME: The Security APIs*. **Volume**,

17. U.S. Government PKE PP with at EAL4 with augmentation (2004) *U.S. Government Family of Protection Profiles for Public Key-Enabled Applications. Volume*,
18. Omar Batarfi. *Certificate Validation in Untrusted Domains*. in *On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops*. 2003. Catania, Sicily, Italy: Springer-Verlag Heidelberg.
19. Compaq Information Technologies Group, L.P., *Compaq Secure Web Server Based on Apache 1.3.26 - SSL User Guide*. 2002: p. 56.
20. The European Commission, *Guidelines, Methodologies and Standards to set up a CA for Digital Signatures*. p. 103.
21. KPMG LLP. *Digital Certificates, Authentication, and Trust on the Internet*. 2002 [cited.
22. Tom Austin, *PKI: A Wiley Tech Brief*. A Wiley Tech Brief, ed. M. Hendrey. 2001: John Wiley & Sons, Inc. 270.
23. T. Klobucar and B. Jerman-Blazic. *A formalisation and evaluation of certificate policies*. 1999 [cited.
24. Athena Bourka, Despina Polemi, and Dimitris Koutsouris. *Certificate Policy Tool for Automated Cross-Certification*,. [cited.
25. Steve Lloyd, *Understanding Certification Path Construction*. 2002. p. 14.
26. Yassir Elley, et al., *Building Certification Paths: Forward vs. Reverse*. p. 8.
27. Whitfield Diffie and Martin E. Hellman. *New Directions in Cryptography*. 1976 [cited.
28. Alexandre R. SILVA and Michael A. STANTON. *Pequi: A PKIX Implementation for Secure Communication*. [cited.
29. Symeon Xenitellis, *The open-source PKI Book: A guide to PKIs and open-source Implementation*. 2000.
30. IETF Secretariat (2006) *Public-Key Infrastructure (X.509) (pkix)*,. **Volume**,
31. Joel Weise. *Public Key Infrastructure Overview*. 2001 [cited.
32. The Institute of Electrical and Electronics Engineers. *IEE Standard Glossary of Computer Applications Terminology*. 1987 [cited.
33. D. Richard Kuhn, et al. *Introduction to Public Key Technology and the Federal PKI Infrastructure*. 2001 [cited; Available from: paper\PKI\Introduction to Public Key.
34. Microsoft TechNet. *Troubleshooting Certificate Status and Revocation*. 2003 [cited; Available from: <http://www.microsoft.com/technet/security/topics/cryptographyetc/tshtcrl.msp> x.
35. Data Connection Ltd. *DIRECTORY SERVICES - THE ROLE OF LDAP AND X.500*. [cited.
36. Carlisle Adams, S.L., *Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition*. SECOND ed. 2003: Addison Wesley. 352.
37. R. Housley, et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280*. 2006 April [cited.
38. Jerilyn Waters. *Digital Certificates*. [cited.
39. Judith V. Boettcher and Amanda Powell. *Digital Certificates What Are They, and What Are They Doing in My Browser?* [cited.
40. D. Olson, *Certificate Authority issues*. 2001.
41. Omar Batarfi. *ATV: An Efficient Method for Constructing a Certification Path*. 2005 [cited.

42. S. Chokhani, et al. *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, RFC 3647*. 2003 November [cited; Available from: c:\paper\cp.
43. Ben Rothke. *THE PROBLEM WITH PKI: AN INSIDER'S VIEW*,. 2001 [cited; Available from: <http://infosecuritymag.techtarget.com/digest/2001/09-06-01.shtml>].
44. American Bar Association. *PKI Assessment Guidelines*. 2001 [cited.
45. American Bar Association. *Digital Signature Guidelines*,. 1996 [cited.
46. Santosh Chokhani. *Certificate Policy Framework*. [cited; Available from: <http://www3.ietf.org/proceedings/97apr/sec/pkix-3/sld001.htm>.
47. COMMERCE NET. *THE HE STRATEGIES TRATEGIES REPORT EPORT*. [cited.
48. EuroPKI Top Level Certification Authority. *EuroPKI Certificate Policy*. [PDF] 2004 [cited; VERSION 1.1:[
49. DevX.com. *XML: Leading the March to Web Services (cont.)*. [cited; Available from: <http://archive.devx.com/javaSR/articles/jones/jones-2.asp>.
50. MSDN. *Importing and Exporting XSD Data in Microsoft Office Access 2003*. [cited; Available from: http://msdn.microsoft.com/library/default.asp?url=/library/en-s/odc_ac2003_ta/html/odc_ac_xsd.asp.
51. S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. 1997 [cited.
52. DutchGrid and NIKHEF. *DutchGrid and NIKHEF - Medium-security X.509 Certification Authority - Certification Policy and Practice Statement*. [PDF] [cited; Version 2.1:[
53. CMS. *Certificate Policy for Digital Signature And Encryption Applications*. [PDF] 2005 [cited; v1.5:[
54. SwUPKI. *Certificate Policy, Digital Signature Medium Strength Soft Certificates*. [PDF] 2001 [cited; Version 1.0:[
55. VeriSign Inc. *VeriSign Trust Network, Certificate Policies*. [PDF] 2005 [cited; Version 2.0:[
56. Shurojit Chatterji and D. Filipovich. *Ambiguous Contracting: Natural Language and Judicial Interpretation*. 2002 [cited.
57. Department of Trade and Industry. *EC DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES*. [PDF] 2001 [cited.
58. C. Adams and S. Farrell. *Internet X.509 Public Key Infrastructure - Certificate Management Protocols*. 2001 [cited.
59. PayPal Inc. *PayPal Buyer Protection Policy*. [cited; Available from: https://www.paypal.com/uk/cgi-bin/webscr?cmd=p/gen/ua/policy_pbp-outside.
60. VISA Inc. *Legal Information*. 1996-2005 [cited; Available from: <http://corporate.visa.com/ut/legal.jsp#Legal>.
61. eBay Inc. *Resolution of Disputes*. 2005 [cited; Available from: <http://pages.ebay.com/help/policies/user-agreement.html>.
62. Queen's Printer of Acts of Parliament. *Data Protection Act 1998*. 1998 [cited; Available from: <http://www.opsi.gov.uk/acts/acts1998/80029--b.htm#7>.
63. the International Organization of Securities Commissions (IOSCO). *PRINCIPLES ON CLIENT IDENTIFICATION AND BENEFICIAL OWNERSHIP FOR THE SECURITIES INDUSTRY*. [PDF] 2004 [cited.

64. State of Washington. *Certificate Policy for the State of Washington Public Key Infrastructure*. [PDF] 2000 [cited].
65. Business Wire. *Face-to-Face Confirmation of Identity for E-Commerce Through Notaries Public to Prevent Identity Theft*. 2001 [cited; Available from: http://www.findarticles.com/p/articles/mi_m0EIN/is_2001_Jan_9/ai_68915878].
66. Working Group on Electronic Commerce and Consumers. *Principles of Consumer Protection for Electronic Commerce - A Canadian Framework*. [PDF] [cited].
67. Peter Gutmann. *PKI: It's Not Dead, Just Resting*. [PDF] 2002 [cited; Available from: <paper\pki\PKI is not dead just resting.pdf>].
68. R. Housley, et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280*. 2002 April [cited].
69. Microsoft TechNet *Revoking certificates and publishing CRLs*. 2005 [cited; Available from: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a4331df0-273b-41a3-95f5-8425d39543c7.mspx>].
70. Roberta Bragg, Mark Rhodes-Ousley, and K. Strassberg, *Network Security: The Complete Reference*. 2003: McGraw-Hill Professional.
71. AMOD PANDIT. *AN INTEGRATED PATTERN RECOGNITION APPROACH FOR ANOMALY DETECTION IN A DISTRIBUTED SYSTEM*. [PDF] 2003 [cited].
72. Computer Security Institute (CSI) and S.F.C.C.S.o.t.F.B.o.I. (FBI). *CSI/FBI 2000 COMPUTER CRIME AND SECURITY SURVEY*. [PDF] 2000 [cited].
73. Communications Electronics Security Group (CESG). *Biometrics and Security - MS04*. [cited; Available from: <http://www.cesg.gov.uk/index.cfm>].
74. Center for Education and Research in Information Assurance and Security (CERIAS). *Threats to Security*. [cited; Available from: http://www.cerias.purdue.edu/education/k-12/cerias_resources/files/infosec_newsletters/03threats.php].
75. DIGITALSIGNATURETRUST. *TrustID Certificate Policy*. [cited; Available from: <http://www.digsigtrust.com/certificates/policy/ts/dst-cp-v20001213.html>].
76. European Grid Authentication Policy Management Authority. *Minimum CA Requirements*. [PDF] 2005 [cited; Available from: <paper\regulation\Minimum CA Requirements.pdf>].
77. Certificate Policy Working Group. *Common Policy Change Proposal*. [pdf] 2005 18 August [cited].
78. Communications-Electronics Security Group (CESG). *CLOUD COVER BASELINE CA PROTECTION PROFILE*. 1999 [cited].
79. John Wack and M. Tracey. *DRAFT Guideline on Network Security Testing - Recommendations of the National Institute of Standards and Technology*. 2001 [cited].
80. VeriSign Inc. *VeriSign Certification Practice Statement*. [PDF] 2002 [cited; Version 2.1,;]
81. European Telecommunications Standards Institute (ETSI). *Policy requirements for certification authorities issuing public key certificates*. [PDF] 2002 [cited].

82. International Organization for Standardization (ISO). *English country names and code elements*. [cited; Available from: <http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html>].
83. Financial Reporting Council (FRC). *AUDIT COMMITTEES COMBINED CODE GUIDANCE*. 2003 [cited; Available from: www.frc.org.uk/publications].
84. Kent Cearley and Lindsay Winsor. *Securing IT Resources with Digital Certificates and LDAP*. 1997 [cited; Available from: <http://www.educause.edu/ir/library/html/cnc9707/cnc9707.html>].
85. EUROPEAN COMMITTEE FOR STANDARDIZATION. *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*. [pdf] 2003 [cited; Available from: paper\regulation\cwa14167-01-2003-Jun.pdf].
86. DOE GRIDS PKI. *DOE Grids Certificate Policy and Certification Practice Statement*. [pdf] 2002 [cited; Version 2.3:[]
87. CESNET. *CESNET CA Certificate Practice Statement*. [cited; Version 1.2:[]
88. Operational Research Consultants (ORC). *Certificate Practice Statement for The Commonwealth of Pennsylvania Department of Environmental Protection*. 2001 [cited].
89. Bill Hayes. *Conducting a Security Audit: An Introductory Overview*. 2003 [cited].
90. National Computational Science Alliance. *National Computational Science Alliance Certificate Policy*. [pdf] 1999 [cited].
91. IUCC Certification Authority. *Certificate Policy and Certification Practice Statement*. 2003 [cited; Available from: paper\CP].
92. CNRS/CNRS-Projets/Datagrid-fr. *Certificate Policy and Certification Practice Statement CNRS/CNRS-Projets/Datagrid-fr*. 2002 [cited].
93. Thomas J. Smedinghoff and M.B. Coles. *Model Certificate Policy*. [pdf] 1998 [cited; Available from: paper\CP].
94. International Organization of Securities Commissions (IOSCO). *PRINCIPLES ON CLIENT IDENTIFICATION AND BENEFICIAL OWNERSHIP FOR THE SECURITIES INDUSTRY*. [PDF] 2004 [cited].
95. U.S. Federal PKI. *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*. [PDF] 2005 [cited; Version 2.3:[]
96. Jens G Jensen. *UK e-Science Certification Authority Certificate Policy and Certification Practices Statement*. 2002 [cited].
97. Federal Bridge Certification Authority (FBCA). *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*. 2006 [cited].
98. VeriSign Inc. *BT Certification Practice Statement*. 2003 [cited; Version 3.04:[]
99. Hungarian National Information Infrastructure (NIIF). *NIIF Certification Authority, Certification Practice Statement (CPS)*. 2005 [cited; Version 1.3:[]
100. Greg Brock. *Implementing Network Security Controls for Intrusion Prevention*. [PDF] 2003 [cited].
101. U.S. Federal Government. *Citizen & Commerce Certificate Policy*. 2002 [cited; Version 1.0:[]
102. UNITED NATIONS (2002) *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*. **Volume**,
103. James Currall. *Digital Signatures: not a solution, simply a link in the process chain*. [PDF] 2002 [cited].

104. Closely Mitrakas. *GlobalSign CA Certificate Policy*. [PDF] 2005 [cited; Version 2.0:]
105. By Kien Keong Wong. *ELECTRONIC COMMERCE LAWS OF SINGAPORE AND MALAYSIA*. 1999 [cited.
106. Carl A. Gunter and Trevor Jim. *Generalized Certificate Revocation*. [cited.
107. Commonwealth of Australia. *Online authentication*. 2002 [cited.
108. United Nations Department of Public Information. *THE UNITED NATIONS: ORGANIZATION*. 2004 [cited; Available from:
<http://www.un.org/aboutun/basicfacts/unorg.htm>.
109. UN Press Release. *Member States of the United Nations*. 2005 [cited; ORG/1360/Rev.1:[Available from:
<http://www.un.org/Overview/unmember.html>.
110. Andreas Mitrakas. *GlobalSign CA Certificate Policy*. [PDF] 2005 [cited; V. 2.0:]
111. John A. Bullinaria. *IAI : Expert Systems*. 2005 [cited.

Appendix A

KEY WORDS FOR USE IN RFCS TO INDICATE REQUIREMENT LEVELS

MUST:

This word, or the terms "REQUIRED" or "SHALL", mean that the

Definition is an absolute requirement of the specification.

MUST NOT:

This phrase, or the phrase "SHALL NOT", mean that the

Definition is an absolute prohibition of the specification.

SHOULD:

This word, or the adjective "RECOMMENDED", mean that there

May exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT:

This phrase, or the phrase "NOT RECOMMENDED" mean that

There may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY:

This word, or the adjective "OPTIONAL", mean that an item is

truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Appendix B

TABLE TO PERFORM A MANUAL COMPARISON

PROCESS

Accordance to the big number of the table pages, we will list only the first seven pages and the full table pages will be included in the attached CD.

EuroPKI	SwuPKI	DutchGrid
1.3 Community and applicability	1.3 Community and Applicability	1.3 Community and Applicability
A conforming CA can choose freely which are the community and applicability of their issued certificates but it MUST clearly specify them in its own CPS. In every case a conforming CA MUST NOT issue certificates to entities that don't belong to its community or for applications that haven't been carefully evaluated (for instance high value B2B transactions). Moreover a conforming CA SHALL respect all the limitations imposed by the following sections of this policy.	This policy is designed for use in SwUPKI. Only Swedish universities or university colleges accredited by the Swedish government and related organisations complying with this CP can be members of SwUPKI. "Organisation" is used to denote a member of SwUPKI.	
	1.3.1 Policy Management Authority (PMA)	
	One member of SwUPKI has the specific responsibility of being the Policy Management Authority of the PKI. The PMA is responsible for: registering, interpreting and maintaining this CP, appointing a member of SwUPKI to serve as the Policy CA for SwUPKI, approving the CPSs of CAs in SwUPKI, compliance inspections and general supervision of SwUPKI, cross-certification with other PKIs and with CAs of other PKIs.	
1.3.1 Certification Authority	1.3.2 Certification Authorities (CAs)	1.3.1 Certification authorities
An issuing conforming CA has to take particular care when it has to decide if a certain organization or individual can manage a subordinate CA performing all the controls and checks detailed in this policy. A conforming CA MAY use as many RAs (registration authorities) as it wishes. A conforming CA MAY also have the role of RA if the entity authentication can be done by the CA itself. Subordinate CAs MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures.	Each Organisation in the PKI shall provide CA services operating in compliance with this CP. Such a CA is responsible for: the creation and signing of certificates, binding Subscribers, PKI personnel and (where permitted) other CAs to the public signature verification keys attributable to them, providing a Certificate Repository and a Certificate Status Service (CSS), see 1.3.4, publishing a CPS that includes reference to this CP, assigning duties to its RAs, and for the compliance with this CP by the CA itself, its RAs and any subordinate CAs. A CA may not assign the duty of issuing certificates to an RA. While an Organisation in the PKI may use a contractor to provide (some of its) CA services, it remains responsible and accountable for the operation of its CA. Cross-certification under this CP, with CAs external to	The only entities that issue certificates of the DutchGrid medium-security Certification Authority are persons, which means that no automated issuing is allowed. These persons are formally assigned staff members responsible for the operational service of the DutchGrid medium-security Certification Authority. The current list of persons comprising the operational staff of the DutchGrid medium-security Certification Authority is published in an on-line accessible repository. The location of this list is stated as part of the CPS in section 1.4. The assigned staff operate the CA functions on a best-effort basis only. The NIKHEF collaboration, the foundation FOM and/or the NIKHEF partners cannot be held liable for any damages resulting from the operation or non-operation of the DutchGrid medium-security Certification Authority. No subordinate certification authorities will be allowed

	SwUPKI, may only be done by the Policy CA after decision by the PMA, and shall comply with this CP and any additional requirements decided by the PMA.	under this policy. Distributed validation will be implemented using a network of trusted registration authorities (RA's).
1.3.2 Registration authorities	1.3.3 Registration Authorities	1.3.2 Registration authorities
<p>Registration Authorities (RA) are needed for physical identification/authentication of entities. These authorities MUST not be permitted to issue certificates.</p> <p>A registration authority (RA) is</p> <ul style="list-style-type: none"> • an individual or • a group of people appointed by an organization or an organizational unit <p>trusted by a CA, serving as a contact point for registration of new end entities, i.e. end entities that want to have a certificate issued. RAs have to check the certificates requester's identity in an appropriate way.</p> <p>The RA MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures.</p>	<p>Any Registration Authority (RA) operating in compliance with this CP is responsible for all duties assigned to it by the CA. An RA may perform duties on behalf of more than one CA, provided that in doing so it satisfies all the requirements of this CP. An RA may not issue certificates.</p>	<p>Individuals or groups of individuals can be recognised by the DutchGrid medium-security Certification Authority to act as trusted intermediaries in the identity verification process between subscriber and certification authority. Such trusted intermediaries are formally assigned by the CA and their identities and contact details published in an on-line accessible repository, the location of which is stated in section 1.4.</p> <p>The RA's are required to sign a document declaring their understanding of and adherence to this CP/CPS.</p>
1.3.3 End entities		1.3.3 End entities
<p>The end entities to be certified under this policy can be a natural person (individual or representing an organization) or a computer entity (e.g. a computer, a router or an application), capable of performing cryptographic operations.</p> <p>Each conforming CA MUST detail in the CPS who are the end entities that it is willing to certify.</p>		<p>Certificates can be issued to natural persons and to computer entities. The entities that are eligible for certification by the DutchGrid medium-security Certification Authority are:</p> <ul style="list-style-type: none"> • all those entities related to organisations, formally based in and/or having offices inside the Netherlands, that are involved in the research or deployment of multi-domain distributed computing infrastructure, intended for cross-organisational sharing of resources. The focus of these organisations should also be in research and/or education. • all those entities associated to the DutchGrid platform. • all organisations located in the "Wetenschappelijk Centrum Watergraafsmeer" in Amsterdam, that are run entirely on a non-for-profit basis.
1.3.4 Applicability	1.3.8 Policy Applicability	1.3.4 Applicability
<p>One of the purposes of this policy is to promote a wide use of public-key certificates in many different applications. In order to promote interoperability this policy strongly encourages CA to support S/MIME for securing e-mail exchanges. It is also suggested that IPsec (to offer network layer security) and SSL/TLS (to offer transport layer security for protecting application protocols like HTTP, Telnet, FTP) SHOULD be supported. It's important to notice that this policy in principle doesn't want to put a priori limitation to the use of the certificates except for the case in which certificates are used in a way that is prohibited by the law of the countries where the issuing CA are established. However in order to evaluate if certificates issued under this policy are suitable for a certain application the chapter 2 about General provisions has to be read carefully and fully understood.</p>	<p>The certificates contain public keys corresponding to private keys for digital signatures. Keys for digital signatures are intended to be used in verification, authentication, data integrity and key agreement mechanisms.</p> <p>The certificates are thus intended to be used for example for verifying the identity of electronic mail correspondents or for remote access to a computer system, verifying the identity of persons or other legal entities, or for protecting the integrity of software and data.</p> <p>The CP is relevant for authentication and the protection of integrity of business transactions within the approval limits of the organisations and such that the falsification of the transaction would cause only minor financial loss or require only administrative action for correction.</p> <p>This limit is at the discretion of the Relying Party or the organisation of the Relying Party.</p> <p>The applicability of certificates issued in compliance with this policy does not rely solely on this compliance but is critically dependent on involved IT-systems as indicated in section 2.1.2.3.</p>	<p>The certificates issued by the DutchGrid medium-security Certification Authority may not be used for financial transactions.</p> <p>Other than that, these certificates may be used for any application that is suitable for X.509 certificates.</p>

	1.3.4 Repositories	
	A CA must ensure that there is a Certificate repository and a Certificate Status Service (CSS) associated with it. A CSS consists of a CRL repository and an optional Online Certificate Status Service (OCSS). These repositories and services shall comply with current standards as stated in the CPS.	
	1.3.5 Sponsors	
	Each Organisation in SwUPKI is solely responsible for issuing the certificates it finds reasons to use in its business. The policy for delegating authority to nominate persons to become Subscribers of certificates will vary between members, but the delegations are given to what we call Sponsors. A Sponsor is an organisational unit or officer with the authority to nominate a person to be a Subscriber of certificates. The Sponsor may suggest appropriate distinguished names for Subjects and is responsible for either supplying or confirming authentication and certificate attribute details to the CA or RA. The Sponsor is also responsible for informing the CA or RA if the sponsor relationship with the Subscriber terminates or changes such that certificates should be revoked. The PMA is the sponsor of the Policy CA.	
	1.3.6 Subscribers	
	A CA may only issue certificates to Subscribers - individuals (employees, students, guests and others) - having a Sponsor within the CA's Organisation. Eligibility for a certificate is at the sole discretion of the CA.	
	1.3.7 Subjects	
	A CA may only issue certificates where the Subject is the Subscriber, or is an organisational role or an IT-system provided that responsibility and accountability is attributable to the Subscriber.	
1.4 Contact Details	1.4 Contact Details	1.4 Contact Details
1.4.1 Specification administration organization		1.4.1 Specification administration organisation
On behalf of EuroPKI this policy is fully managed by the Computer and Network Security Group (CNSG) of Politecnico di Torino, Italy (http://security.polito.it/).	This Certificate Policy is registered by Stockholms universitet, SE 106 91 Stockholm, Sweden. Stockholms universitet is the PMA of this SwUPKI CP and is fully responsible for registration, maintenance, and interpretation of the policy. Questions concerning this policy should be addressed to: SwUPKI, Enheten för IT och Media, Stockholms universitet, SE 106 91 Stockholm, Sweden or info@swupki.su.se . As an alternative to the address above, potential members may address their inquiries and requests to request@swupki.su.se or access http://www.swupki.su.se/join.html .	The DutchGrid medium-security Certification Authority is administered by the Dutch "Nationaal Instituut voor Kernfysica en Hoge-Energie Fysica (NIKHEF)" as part of its DataGrid project effort by David Groep. It is operated by the NIKHEF Computer Technology Group (CT). The contact person for this CP/CPS is: David Groep, DutchGrid and NIKHEF CA operations, P.O. Box 41882, NL-1009 DB Amsterdam, The Netherlands phone: +31 20 592 2179, telefax: +31 20 592 5155, telex: 10262 hef nl e-mail: ca@nikhef.nl .
		1.4.1.1 Online repositories
		general web address http://certificate.nikhef.nl/policy/documents http://certificate.nikhef.nl/medium/policy/ certificate repository http://certificate.nikhef.nl/medium/

		<p>ldap://certificate.nikhef.nl/o=dutchgrid</p> <p>certificate revocation list http://certificate.nikhef.nl/medium/cacrl.pem</p> <p>root certificate http://certificate.nikhef.nl/medium/cacert.pem</p>
1.4.2 Contact person		1.4.2 Contact person
<p>Contact point for questions related to this policy is:</p> <p>Address Prof. Antonio Lioy EuroPKI Root Certification Authority c/o Politecnico di Torino Dip. Automatica e Informatica corso Duca degli Abruzzi, 24 10129 Torino (Italy)</p> <p>Phone +39 0115647021 / +39 0115647054 Fax +39 0115647099 URI http://www.europki.org/ca/root/ e-mail ca@europki.org</p>		<p>The DutchGrid medium-security Certification Authority is operated (as meant by section 1.3.1) by:</p> <ul style="list-style-type: none"> • David Groep, NIKHEF, phone +31 20 592 2179 • Djuhaeri Harapan, NIKHEF, phone +31 20 592 2139 <p>The Registration Authorities for the DutchGrid medium-security Certification Authority are:</p> <ul style="list-style-type: none"> • David Groep, NIKHEF, phone +31 20 592 2179 • Djuhaeri Harapan, NIKHEF, phone +31 20 592 2139 • Zeger Hendrikse, University of Amsterdam Informatics Institute, phone: +31 20 525 7535
1.4.3 Person determining CPS suitability for the policy		1.4.3 Person determining CPS suitability for the policy

Appendix C

UNCITRAL MODEL LAW ON ELECTRONIC

SIGNATURES (2001)

Article 1. Sphere of application

This Law applies where electronic signatures are used in the context of commercial activities. It does not override any rule of law intended for the protection of consumers.

Article 2. Definitions

For the purposes of this Law:

- (a)* “Electronic signature” means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message;
- (b)* “Certificate” means a data message or other record confirming the link between a signatory and signature creation data;
- (c)* “Data message” means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts either on its own behalf or on behalf of the person it represents;
- (d)* “Signatory” means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
- (e)* “Certification service provider” means a person that issues certificates and may provide other services related to electronic signatures;
- (f)* “Relying party” means a person that may act on the basis of a certificate or an electronic signature.

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the

requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law.

Article 4. Interpretation

1. In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

2. Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Article 6. Compliance with a requirement for a signature

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].

Article 7. Satisfaction of article 6

1. *[Any person, organ or authority, whether public or private, specified by the enacting State as competent]* may determine which electronic signatures satisfy the provisions of article 6 of this Law.

2. Any determination made under paragraph 1 shall be consistent with recognized international standards.

3. Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) The signatory knows that the signature creation data have been compromised; or

(ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 9. Conduct of the certification service provider

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) Act in accordance with representations made by it with respect to its policies and practices;

(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:

(i) The identity of the certification service provider;

(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) That signature creation data were valid at or before the time when the certificate was issued;

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) The method used to identify the signatory;

(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) That the signature creation data are valid and have not been compromised;

(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law;

(vi) Whether a timely revocation service is offered;

(e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;

(f) Utilize trustworthy systems, procedures and human resources in performing its services.

3. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 10. Trustworthiness

For the purposes of article 9, paragraph 1 (*f*), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

- (a) Financial and human resources, including existence of assets;
- (b) Quality of hardware and software systems;
- (c) Procedures for processing of certificates and applications for certificates and retention of records;
- (d) Availability of information to signatories identified in certificates and to potential relying parties;
- (e) Regularity and extent of audit by an independent body;
- (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
- (g) Any other relevant factor.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure:

- (a) To take reasonable steps to verify the reliability of an electronic signature; or
- (b) Where an electronic signature is supported by a certificate, to take reasonable steps:
 - (i) To verify the validity, suspension or revocation of the certificate; and
 - (ii) To observe any limitation with respect to the certificate.

Article 12. Recognition of foreign certificates and electronic signatures

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

(a) To the geographic location where the certificate is issued or the electronic signature created or used; or

(b) To the geographic location of the place of business of the issuer or signatory.

2. A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.

3. An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.

5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

Appendix D

CRITERIA XML FORMALISATION

```
<?xml version="1.0"?>
<criteria xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="file:///d:/Academic/XML
L-CP/final/criteria-schema.xsd">

  <Criterion1>
    <CertificationAuthority>
      <requirement>
        <checking>
          <capability of="subject" toManage="subordinate CA">
            <requirement>
              <withCompliance with="agreed CP"/>
            </requirement>
          </capability>
        </checking>
      </requirement>
    </CertificationAuthority>
  </Criterion1>

  <critrion2>
    <RegistrationAuthority>
      <prohibition>
        <issue>
          <certificates to="subject"/>
        </issue>
      </prohibition>
    </RegistrationAuthority>
  </critrion2>

  <critrion3>
    <participant>
      <requirement>
        <declare>
          <financialResponsibility for="its liabilities" to="other participants"/>
          <assets to="support its operations and liabilities"/>
        </declare>
      </requirement>
    </participant>
  </critrion3>

  <Criterion4>
    <CertificationAuthority>
      <requirement>
        <ensure>
          <law ofCountry="ISO country name" governsAnyAgreement="true">
            <requirement>
              <sameCountry where="CA" isEstablished="true"/>
            </requirement>
          </law>
        </ensure>
      </requirement>
    </CertificationAuthority>
  </Criterion4>

  <Criterion5>
    <CertificationAuthority>
      <requirement>
        <allow>
```

```

        <arbitration to="resolve disputes arising out of its CP"/>
    </allow>
</requirement>
</CertificationAuthority>
</Criterion5>

<Criterion6>
    <CertificationAuthority>
        <requirement>
            <perform>
                <process of="complianceAudit">
                    <requirement>
                        <carryOut by="external auditor"/>
                    </requirement>
                </process>
            </perform>
        </requirement>
    </CertificationAuthority>
</Criterion6>

<Criterion7>
    <CertificationAuthority>
        <requirement>
            <run>
                <complianceAudit>
                    <requirement>
                        <annually atLeast="1"/>
                    </requirement>
                </complianceAudit>
            </run>
        </requirement>
    </CertificationAuthority>
</Criterion7>

<Criterion8>
    <CertificationAuthority>
        <requirement>
            <revoke>
                <subjectCertificate to="certificate revocation list">
                    <requirement>
                        <subjectOperation complyWithCP="false"/>
                    </requirement>
                </subjectCertificate>
            </revoke>
        </requirement>
    </CertificationAuthority>
</Criterion8>

<Criterion9>
    <CertificationAuthority>
        <prohibition>
            <discloseTo>
                <thirdParties any="confidential information" of="subject">
                    <requirement>
                        <except>
                            <whenRequestedByLaw>true</whenRequestedByLaw>
                            <whenConsentBySubject>true</whenConsentBySubject>
                        </except>
                    </requirement>
                </thirdParties>
            </discloseTo>
        </prohibition>
    </CertificationAuthority>
</Criterion9>

<Criterion10>
    <RegistrationAuthority>

```



```

    <requirement>
      <authenticate>
        <organization include="its reputation"/>
      </authenticate>
    </requirement>
  </RegistrationAuthority>
</Criterion10>

<Criterion11>
  <RegistrationAuthority>
    <requirement>
      <authenticate>
        <individual basedOn="its physical presence"/>
      </authenticate>
    </requirement>
  </RegistrationAuthority>
</Criterion11>

<Criterion12>
  <CertificationAuthority>
    <requirement>
      <insure>
        <subject isAwareOf="its respective rights and obligations"/>
      </insure>
    </requirement>
  </CertificationAuthority>
</Criterion12>

<Criterion13>
  <CertificationAuthority>
    <requirement>
      <update>
        <CRL after="every certificate revocation">
          <requirement>
            <updateIntervalTime withIn="1 hour"/>
          </requirement>
        </CRL>
      </update>
    </requirement>
  </CertificationAuthority>
</Criterion13>

<Criterion14>
  <CertificationAuthority>
    <requirement>
      <publish>
        <CRL>
          <requirement>
            <intervalTime withIn="30 days"/>
          </requirement>
        </CRL>
      </publish>
    </requirement>
  </CertificationAuthority>
</Criterion14>

<Criterion15>
  <CertificationAuthority>
    <requirement>
      <do>
        <securtyAudit>
          <requirement>
            <allBootsOfThePKIsystem>true</allBootsOfThePKIsystem>
            <allAccessAttemptsToPKIsystem>true</allAccessAttemptsToPKIsystem>
            <allPKIsystemFailures>true</allPKIsystemFailures>
            <CAkeyGeneration>true</CAkeyGeneration>
            <CAkeyStorage>true</CAkeyStorage>
          </requirement>
        </securtyAudit>
      </do>
    </requirement>
  </CertificationAuthority>
</Criterion15>

```

```

    <CAkeyBackup>true</CAkeyBackup>
    <CAkeyArchival>true</CAkeyArchival>
    <CAkeyRecovery>true</CAkeyRecovery>
    <CAkeyDestruction>true</CAkeyDestruction>
    <CAandSubjectCertificate>
      <generationRequests>true</generationRequests>
      <renewalRequests>true</renewalRequests>
      <re-keyRequests>true</re-keyRequests>
      <revocationRequests>true</revocationRequests>
    </CAandSubjectCertificate>
    <issuanceOfCertificates>true</issuanceOfCertificates>
    <certificateRequests>
      <ofStatusChange>true</ofStatusChange>
      <ofStatus>true</ofStatus>
      <responses>true</responses>
    </certificateRequests>
    <PKIandSecuritySystemActions>
      <performedByCApersonnel>true</performedByCApersonnel>
    </PKIandSecuritySystemActions>
    <identityVerificationProcedures>true</identityVerificationProcedures>
  </requirement>
</securtyAudit>
</do>
</requirement>
</CertificationAuthority>
</Criterion15>

<Criterion16>
  <CertificationAuthority>
    <requirement>
      <examine>
        <auditLogs>
          <requirement>
            <frequent atLeast="weekly"/>
          </requirement>
        </auditLogs>
      </examine>
    </requirement>
  </CertificationAuthority>
</Criterion16>

<Criterion17>
  <CertificationAuthority>
    <requirement>
      <execute>
        <process of="vulnerability assessments"/>
      </execute>
    </requirement>
  </CertificationAuthority>
</Criterion17>

<Criterion18>
  <CertificationAuthority>
    <requirement>
      <provide>
        <archiving>
          <requirement>
            <certificateRequestApplication>true</certificateRequestApplication>
            <documentationSupportingCertificateApplications>true</documentationSupportingCertificateApplications>
            <allComputerSecurityAuditData>true</allComputerSecurityAuditData>
            <certificateRevocationApplication>true</certificateRevocationApplication>
            <certificateRe-keyApplication>true</certificateRe-keyApplication>
            <certificateRenewalApplication>true</certificateRenewalApplication>
            <issuedCertificates>true</issuedCertificates>
            <issuedCRLsORcertificateStatusRecords>true</issuedCRLsORcertificateStatusRecords>
            <allcorrespondence>
              <betweenTheCAandSubcontractors>true</betweenTheCAandSubcontractors>
            </allcorrespondence>
          </requirement>
        </archiving>
      </provide>
    </requirement>
  </CertificationAuthority>
</Criterion18>

```



```

        <betweenTheCAandSubscribers>true</betweenTheCAandSubscribers>
    </allcorrespondence>
    <retentionPeriod>
        <requirement>
            <atLeast In Years="5"/>
        </requirement>
    </retentionPeriod>
</requirement>
</archiving>
</provide>
</requirement>
</CertificationAuthority>
</Criterion18>

<Criterion19>
    <CertificationAuthority>
        <requirement>
            <establish>
                <plan of="surviving after the disaster"/>
            </establish>
        </requirement>
    </CertificationAuthority>
</Criterion19>

<Criterion20>
    <CertificationAuthority>
        <requirement>
            <support>
                <trustedRoles>
                    <requirement>
                        <securityOfficers>true</securityOfficers>
                        <registrationOfficers>true</registrationOfficers>
                        <syemAdministrators>true</syemAdministrators>
                        <systemOperators>true</systemOperators>
                        <systemAuditors>true</systemAuditors>
                    </requirement>
                </trustedRoles>
            </support>
        </requirement>
    </CertificationAuthority>
</Criterion20>

<Criterion21>
    <CertificationAuthority>
        <requirement>
            <assure>
                <allPersonneControlled>
                    <requirement>
                        <backgroundChecked>
                            <qualifications>true</qualifications>
                            <experience>true</experience>
                            <governmentClearances>true</governmentClearances>
                        </backgroundChecked>
                        <providingWthTaining>true</providingWthTaining>
                        <povidingWthRefresherTaining>true</povidingWthRefresherTaining>
                        <sanctioningForUnauthorizedActions>true</sanctioningForUnauthorizedActions>
                        <providingWithDocumentation>true</providingWithDocumentation>
                    </requirement>
                </allPersonneControlled>
            </assure>
        </requirement>
    </CertificationAuthority>
</Criterion21>

<Criterion22>
    <subject>
        <requirement>

```

```

    <generate>
      <itsKeys>true</itsKeys>
    </generate>
  </requirement>
</subject>
</Criterion22>

<Criterion23>
  <CertificationAuthority>
    <requirement>
      <makeSure>
        <minimumLength of="private key" isInBits="1024"/>
      </makeSure>
    </requirement>
  </CertificationAuthority>
</Criterion23>

<Criterion24>
  <CertificationAuthority>
    <prohibition>
      <create>
        <CAcertificateValidityPeriods moreThanInYears="20"/>
        <subjectCertificateValidityPeriods moreThanInYear="1"/>
      </create>
    </prohibition>
  </CertificationAuthority>
</Criterion24>

<Criterion25>
  <CertificationAuthority>
    <requirement>
      <secure>
        <CAmachine>
          <requirement>
            <disconnectFromNetwork>true</disconnectFromNetwork>
            <prohibitUnauthorizedAccess>true</prohibitUnauthorizedAccess>
            <updatingOSwithSecurityPatches>true</updatingOSwithSecurityPatches>
            <limitAccess>true</limitAccess>
          </requirement>
        </CAmachine>
      </secure>
    </requirement>
  </CertificationAuthority>
</Criterion25>

<Criterion26>
  <CertificationAuthority>
    <requirement>
      <examining>
        <integrityOfHardwareAndSoftwareBy>
          <requirement>
            <documentedAndControlledAny>
              <configuration>true</configuration>
              <modifications>true</modifications>
              <upgrades>true</upgrades>
            </documentedAndControlledAny>
            <detectingUnauthorizedModification>true</detectingUnauthorizedModification>
            <checkingSoftwareIntegrity>
              <requirement>
                <atLeast inDays="7"/>
              </requirement>
            </checkingSoftwareIntegrity>
          </requirement>
        </integrityOfHardwareAndSoftwareBy>
      </examining>
    </requirement>
  </CertificationAuthority>

```



```
</Criterion26>
<Criterion27>
  <CertificationAuthority>
    <requirement>
      <securing>
        <networks>
          <requirement>
            <firewalls>true</firewalls>
            <encryptionAndDigitalSignatures>true</encryptionAndDigitalSignatures>
            <ACLs>true</ACLs>
          </requirement>
        </networks>
      </securing>
    </requirement>
  </CertificationAuthority>
</Criterion27>
</criteria>
```